Singularities of Plane Algebraic Curves

Robert Härkönen

August 2021

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

MATEMAATTIS-LUONNONTIETEELLINEN TIEDEKUNTA
MATEMATISK-NATURVETENSKAPLIGA FAKULTETEN
FACULTY OF SCIENCE

Tiedekunta – Fakultet – Faculty		Koulutusohjelma – Utbildningsprogram – Degree programme
Faculty of Science		Master's Programme in Mathematics and Statistics
Opintosuunta – Studieinrikting – Study track		
Geomtery, Algebra and Topology		
Tekijä – Författare – Author		
Robert Härkönen		
Työn nimi – Arbetets titel – Title		
Singularities of Plane Algebraic Curves		
Työn laji – Arbetets art – Level	Aika – Datum – Month and year	Sivumäärä – Sidoantal – Number of pages
Master's Thesis	August 2021	42

Tiivistelmä – Referat – Abstract

Plane algebraic curves are defined as zeroes of polynomials in two variables over some given field. If a point on a plane algebraic curve has a unique tangent line passing through it, the point is called simple. Otherwise, it is a singular point or a singularity. Singular points exhibit very different algebraic and topological properties, and the objective of this thesis is to study these properties using methods of commutative algebra, complex analysis and topology.

In chapter 2, some preliminaries from classical algebraic geometry are given, and plane algebraic curves and their singularities are formally defined. Curves and their points are linked to corresponding coordinate rings and local rings. It is shown that a point is simple if and only if its corresponding local ring is a discrete valuation ring.

In chapter 3, the Newton-Puiseux algorithm is introduced. The algorithm outputs fractional power series known as Puiseux expansions, which are shown to produce parametrizations of the local branches of a curve around a singular point.

In chapter 4, Puiseux expansions are used to study the topology of complex plane algebraic curves. Around singularities, curves are shown to have an iterated torus knot structure which is, up to homotopy, determined by invariants known as Puiseux pairs.

Avainsanat – Nyckelord – Keywords

singularity, plane curve, Puiseux, torus knot

Säilytyspaikka – Förvaringställe – Where deposited

sähköinen arkisto

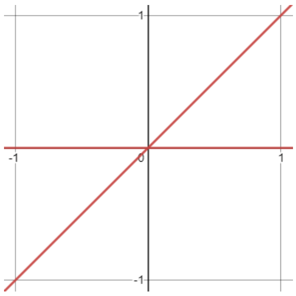
Muita tietoja – Övriga uppgifter – Additional information

Contents

1 Introduction

Plane algebraic curves are defined as the zeroes of polynomials in two variables. Most points on such curves are *simple*: they have a unique tangent line passing through them. Points that are not simple are called *singular*, and such points exhibit very different algebraic properties, via the so-called local rings of the curve, and topological properties, via the behaviour of the curve in a small neighbourhood of the singularity. In this thesis, we investigate these properties using some methods of commutative algebra, complex analysis, and topology. The main result of this thesis is the Newton-Puiseux algorithm covered in section 3.2.

As an easy example, the curve given by the polynomial $f = Y^2 - XY = Y(Y - X)$ is the union of the X-axis and the line $Y = X$. The origin is a singular point: the curve locally branches along the two different lines. Every other point is simple and has a unique tangent line passing through it.



A sufficient prerequisite knowledge to comfortably read this thesis should be given by the courses *Algebra II*, *Topology II* and *Complex analysis I* at the University of Helsinki.

In Chapter 2, we define affine algebraic sets and curves and their associated coordinate rings, rational function fields, and local rings. Singular points are introduced, and we show that a point being singular or not determines the behaviour of the local ring at that point. This is formulated precisely in Theorem 2.3.1, which is the main goal of this chapter. An important subgoal is showing that the local ring is preserved under a change of coordinates: this is Lemma 2.3.4.

In Chapter 3, we construct the so-called Puiseux expansion of a curve, using an algorithm known as the Newton-Puiseux algorithm (Theorem 3.2.1). This produces local parametrizations of the branches of a curve; we move from an implicitly defined curve as zeroes of a polynomial, to an explicit expression using fractional power series. The algorithm is analyzed further in section 3.3, showing how all branches can be found and that the power series output by the algorithm are convergent over C.

In Chapter 4, Puiseux expansions are used to construct braids of curves in small neighbourhoods of singular points. The main goal of this chapter is Theorem 4.2.3, in which the topology of these braids is shown to classify singularities of irreducible curves using invariants known as Puiseux pairs.

2 Singularities of plane curves

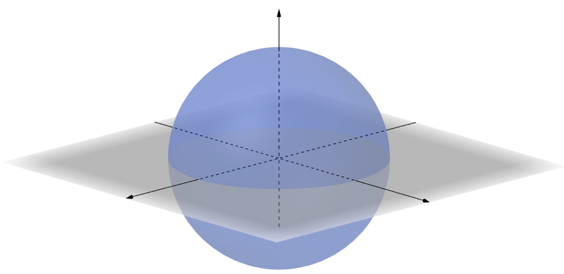
Throughout this chapter, let k be an algebraically closed field. We will often take $k = \mathbb{C}$ to aid in illustrations, but the constructions and results here will hold for general k. The notation and results presented here will be largely based on those found in [9] and [2].

2.1 Affine algebraic sets and coordinate rings

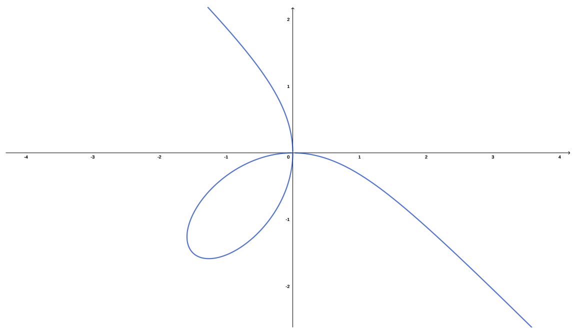
We denote by $\mathbb{A}^n(k) := k^n$ the *n-dimensional affine space over k*. Any polynomial $p \in k[X_1, \ldots, X_n]$ defines a map $p : \mathbb{A}^n \to \mathbb{A} = k$ in the natural way. For a subset of polynomials $P \subseteq k[X_1, \ldots, X_n]$, the set

$$\mathcal{V}(P) = \{a \in \mathbb{A}^n \mid p(a) = 0 \ \forall p \in P\}$$

is called the *affine algebraic set defined by P*. It is the zero set, or zero-locus, of the polynomials in P. A set $V \subseteq \mathbb{A}^n$ is an *affine algebraic set*, or simply *algebraic set*, if $V = \mathcal{V}(P)$ for some $P \subseteq k[X_1, \ldots, X_n]$. It is easy to see that $\mathcal{V}(P) = \mathcal{V}(I)$, where I is the ideal generated by P. From here on, if $\{p_1, \ldots, p_m\}$ are polynomials, we will simply write $\mathcal{V}(p_1, \ldots, p_m)$ instead of $\mathcal{V}(\{p_1, \ldots, p_m\})$.



$\mathcal{V}(X_1^2 + X_2^2 + X_3^2 - 1)$, *the usual 3-sphere*



$\mathcal{V}(X_1^3 + X_2^3 - 3X_1X_2)$

In the above figures, we have plotted the real parts of two algebraic sets over $\mathbb{C}$. This does not give the full picture: for instance $\mathcal{V}(X_1^2 + X_2^2 + 1)$ would appear empty in the real plane, but contains the point $(i, 0)$.

The following properties will be useful.

Lemma 2.1.1. *Let $I_1, I_2 \subseteq k[X_1, \ldots, X_n]$ be ideals.*

1. $I_1 \subseteq I_2 \implies \mathcal{V}(I_2) \subseteq \mathcal{V}(I_1)$
2. $\mathcal{V}(I_1) \cup \mathcal{V}(I_2) = \mathcal{V}(I_1 \cap I_2) = \mathcal{V}(I_1 I_2)$

Proof. 1. Let $a \in \mathcal{V}(I_2)$. For every $p \in I_1$, $p \in I_2$ by assumption so p vanishes on a, i.e. $a \in \mathcal{V}(I_1)$.

2. Note that $I_1 I_2 \subseteq I_1 \cap I_2 \subseteq I_j$ for $j = 1, 2$. By part 1, the inclusions "$\supseteq$" hold. Next we show that $\mathcal{V}(I_1 I_2) \subseteq \mathcal{V}(I_1) \cup \mathcal{V}(I_2)$. Suppose $a \in \mathcal{V}(I_1 I_2)$ and $a \notin \mathcal{V}(I_1)$. There exists some $p_1 \in I_1$ s.t. $p_1(a) \neq 0$. Now let $p_2 \in I_2$ be arbitrary, then $p_1 p_2 \in I_1 I_2$ and $p_1 p_2(a) = 0 = p_1(a) p_2(a)$. Because $p_1(a) \neq 0$ and we are in a field, it follows that $p_2(a) = 0$ for all $p_2 \in I_2$, i.e. $a \in \mathcal{V}(I_2)$. So whether or not $a \in \mathcal{V}(I_1)$ holds, we get $a \in \mathcal{V}(I_1) \cup \mathcal{V}(I_2)$.

□

Just how ideals in $k[X_1, \ldots, X_n]$ define algebraic sets in $\mathbb{A}^n$, there is an inverse operation taking algebraic sets to ideals of polynomials. If $V \subseteq \mathbb{A}^n$ is an algebraic set, then define

$$\mathcal{I}(V) := \{p \in k[X_1, \ldots, X_n] \mid p(a) = 0 \ \forall a \in V\}$$

to be the *vanishing ideal* of V. We show some useful properties of these:

Lemma 2.1.2. *Let $V_1, V_2 \subseteq \mathbb{A}^n$ be algebraic sets.*

1. *If $V_1 \subseteq V_2$, then $\mathcal{I}(V_2) \subseteq \mathcal{I}(V_1)$.*
2. *$\mathcal{I}(V_1 \cup V_2) = \mathcal{I}(V_1) \cap \mathcal{I}(V_2)$*
3. *$\mathcal{V}(\mathcal{I}(V_1)) = V_1$*

Proof. 1. Let $p \in \mathcal{I}(V_2)$. Then p vanishes on V_2 and hence on the subset V_1, so $p \in \mathcal{I}(V_1)$.

2. It holds $p \in \mathcal{I}(V_1 \cup V_2)$ iff p vanishes on $V_1 \cup V_2$ iff p vanishes on V_1 and on V_2 iff $p \in \mathcal{I}(V_1) \cap \mathcal{I}(V_2)$.

3. Let $V = \mathcal{V}(I_1)$, for $I_1 \in k[X_1, \ldots, X_n]$ an ideal. Then $I_1 \subseteq \mathcal{I}(V)$ by definition, so by Lemma 2.1.1, $\mathcal{V}(\mathcal{I}(V)) \subseteq \mathcal{V}(I_1) = V$. Conversely, $V \subseteq \mathcal{V}(\mathcal{I}(V))$ is clear.

□

The famous *Nullstellensatz* shows how algebraic sets and vanishing ideals interact. We will only use it briefly; a proof is given by e.g. Fulton or Kunz.

Theorem 2.1.3 (Hilbert's Nullstellensatz)**.** *If $I \subseteq k[X_1, \ldots, X_n]$ is an ideal, then $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$, where*

$$\sqrt{I} = \{p \in k[X_1, \ldots, X_n] \mid p^n \in I \text{ for some } n \in \mathbb{N}\}$$

is the radical of I.

Proof. Cf. [9] or [2]. □

An algebraic set $V \subseteq \mathbb{A}^n$ is *reducible*, if there exist algebraic sets $V_1, V_2 \subseteq \mathbb{A}^n$ such that $V = V_1 \cup V_2$, and $V \neq V_1$, $V \neq V_2$. If V is not reducible, it is *irreducible*. If an affine algebraic set is irreducible, we call it an *affine variety*, or simply *variety*.

Proposition 2.1.4. *An algebraic set $V \subseteq \mathbb{A}^n$ is irreducible if and only if $\mathcal{I}(V) \subseteq k[X_1, \ldots, X_n]$ is a prime ideal.*

Proof. Let V be irreducible. Let $p, q \in k[X_1, \ldots, X_n]$ such that $pq \in \mathcal{I}(V)$. Then $V \subseteq \mathcal{V}(pq) = \mathcal{V}(p) \cup \mathcal{V}(q)$, i.e. $V = (\mathcal{V}(p) \cap V) \cup (\mathcal{V}(q) \cap V)$ as a union of algebraic sets. By irreducibility, it follows $V = \mathcal{V}(p) \cap V$ or $V = \mathcal{V}(q) \cap V$. Now either p or q vanishes on V, so $p \in \mathcal{I}(V)$ or $q \in \mathcal{I}(V)$, and $\mathcal{I}(V)$ is prime.

Let $\mathcal{I}(V)$ be prime, and suppose $V = V_1 \cup V_2$. Now $\mathcal{I}(V) = \mathcal{I}(V_1) \cap \mathcal{I}(V_2)$. Because $\mathcal{I}(V_1)\mathcal{I}(V_2) \subseteq \mathcal{I}(V_1) \cap \mathcal{I}(V_2) = \mathcal{I}(V)$, it follows $\mathcal{I}(V_1) \subseteq \mathcal{I}(V)$ or $\mathcal{I}(V_2) \subseteq \mathcal{I}(V)$ since $\mathcal{I}(V)$ is prime, and hence $\mathcal{I}(V) = \mathcal{I}(V_1)$ or $\mathcal{I}(V) = \mathcal{I}(V_2)$. Now either $V = \mathcal{V}(\mathcal{I}(V)) = \mathcal{V}(\mathcal{I}(V_1)) = V_1$ or $V = \mathcal{V}(\mathcal{I}(V)) = \mathcal{V}(\mathcal{I}(V_2)) = V_2$, so V is irreducible. □

Let V be a nonempty variety. Suppose we want to define polynomial functions $p : V \to \mathbb{A}$. We could restrict polynomials $p, q \in k[X_1, \ldots, X_n]$ to V, but would soon notice that the polynomials no longer define unique maps. We note that $p(x) = q(x)$ for all $x \in V$ if and only if $p(x) - q(x) = (p - q)(x) = 0$ for all $x \in V$. In other words, $p - q \in \mathcal{I}(V)$, and we could say that $p = q$ modulo $\mathcal{I}(V)$. Because V is a variety, $\mathcal{I}(V)$ is a prime ideal by Proposition 2.1.4. Then

$$\Gamma(V) := k[X_1, \ldots, X_n]/\mathcal{I}(V)$$

is an integral domain, called the *coordinate ring* of V.

If R is an integral domain, we can define its *field of fractions*, denoted $\mathrm{Frac}(R)$. It consists of equivalence classes of pairs (a, b), $a, b \in R, b \neq 0$ and where $(a, b) \equiv (c, d)$ if and only if $ad = bc$. These equivalence classes are written $\frac{a}{b}$ for short, and follow the expected rules of addition and multiplication: $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ and $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$. We can embed R into $\mathrm{Frac}(R)$ in a natural way by mapping a to $\frac{a}{1}$.

Now if $V \subseteq \mathbb{A}^n$ is a variety with coordinate ring $\Gamma(V)$, then we define $k(V) := \mathrm{Frac}(\Gamma(V))$ as the *field of rational functions* on V. Because the elements of $\Gamma(V)$ correspond to polynomial functions on V, we call elements of $k(V)$ *rational functions* on V. A rational function $f \in k(V)$ is defined at $P \in V$, if there exist $a, b \in \Gamma(V)$ s.t. $f = \frac{a}{b}$ and $b(P) \neq 0$.

For $P \in V$, define

$$\mathcal{O}_P(V) := \{f \in k(V) \mid f \text{ is defined at } P\}.$$

This is called the *local ring of V at P*. The set $\mathcal{O}_P(V)$ is indeed a ring: if $\frac{f}{g}, \frac{s}{t} \in \mathcal{O}_P(V)$, then $g(P), t(P) \neq 0$ and hence $g(P)t(P) \neq 0$ (a field does not have zero divisors). Then $\frac{ft+sg}{gt}$ and $\frac{fs}{gt}$ are defined at P, which shows $\mathcal{O}_P(V)$ to be closed under sums and products. Further, $0, 1 \in \mathcal{O}_P(V)$ and additive inverses are also defined at P, so $\mathcal{O}_P(V)$ is a ring. Further, it holds $\Gamma(V) \subseteq \mathcal{O}_P(V) \subseteq k(V)$: the second inclusion by definition, and the first since for $f \in \Gamma(V)$, $\frac{f}{1}$ is defined at P.

Lemma 2.1.5. *Let R be a ring. The following are equivalent:*

1. *The non-units of R form an ideal.*

2. *There is a unique maximal ideal I of R such that every proper ideal of R is contained in I.*

A ring satisfying these conditions is called a ***local ring****.*

Proof. Denote $\mathfrak{m} = \{a \in R \mid a \text{ is not a unit}\}$. Because an ideal containing a unit would be the whole ring R, any proper ideal of R does not contain units and is thus contained in $\mathfrak{m}$. This shows $1 \implies 2$. In the other direction, let I be the unique maximal ideal. Now $I \subseteq \mathfrak{m}$ because I contains only non-units, and $\mathfrak{m} \subseteq I$ since for a non-unit a, (a) is a proper ideal. Thus $\mathfrak{m} = I$ is an ideal. □

The ring $\mathcal{O}_P(V)$ is also a local ring in the above definition. We may define the *evaluation homomorphism* $\phi_P : \mathcal{O}_P(V) \to k, \phi_P(f) = f(P) = \frac{a(P)}{b(P)}$, where $b(P) \neq 0$. This homomorphism is surjective and has kernel

$$\mathfrak{m}_P(V) := \{f \in \mathcal{O}_P(V) \mid f(P) = 0\},$$

so by the first isomorphism theorem, $\mathcal{O}_P(V)/\mathfrak{m}_P(V)$ is isomorphic to k. But since k is a field, this means that $\mathfrak{m}_P(V)$ is a maximal ideal of $\mathcal{O}_P(V)$. If $f = \frac{a}{b} \in \mathcal{O}_P(V)$ is nonzero at P, then $a(P), b(P) \neq 0$, and f has inverse $g = \frac{b}{a} \in \mathcal{O}_P(V)$. Conversely, if $f(P) = 0$, then $(f \cdot g)(P) = 0$ for every $g \in \mathcal{O}_P(V)$ so f is a non-unit. We conclude that $\mathfrak{m}_P(V)$ contains exactly the non-units, so $\mathcal{O}_P(V)$ is a local ring in the above definition.

A *Noetherian ring* is a ring whose every ideal is finitely generated. In particular, fields and principal ideal domains (PIDs) are Noetherian. We will use the following well-known result about Noetherian rings:

Theorem 2.1.6 (Hilbert's Basis Theorem)**.** *If R is a Noetherian ring, so is the polynomial ring $R[X_1, \dots, X_n]$.*

Proof. Cf. Fulton [9] or Kunz [2]. □

We see that $k[X_1, \dots, X_n]$ is Noetherian because k is a field. It turns out quotient rings of Noetherian rings are themselves always Noetherian, which we prove as follows. Let R be a Noetherian ring, I an ideal of R, and J an ideal of R/I. The quotient map $\pi : R \to R/I$ is a homomorphism, so the preimage $\pi^{-1}(J)$ is an ideal in R and hence has generators $x_1, \dots, x_m$. Now for any $b \in J$, there exists $a = \sum_{i=1}^m a_i x_i \in \pi^{-1}(J)$ with $b = \pi(a) = \sum_{i=1}^m \pi(a_i)\pi(x_i)$, whereby J is generated by $\pi(x_1), \dots, \pi(x_m)$.

As an immediate result of this, the coordinate ring $\Gamma(V)$ is Noetherian. What about the local rings?

Proposition 2.1.7. *$\mathcal{O}_P(V)$ is a Noetherian ring.*

Proof. Let $I \subseteq \mathcal{O}_P(V)$ be an ideal. Then $I \cap \Gamma(V)$ is an ideal of $\Gamma(V)$ and has generators $p_1, \dots, p_n$ since $\Gamma(V)$ is noetherian. Then for $q \in I$, there exist $a, b \in \Gamma(V)$ for which $q = \frac{a}{b}$, $b(P) \neq 0$. But now $bq \in I \cap \Gamma(V)$, so we get a representation $bq = \sum_{i=1}^n a_i p_i$ with $a_i \in \Gamma(V)$. Now $\frac{a_i}{b} \in \mathcal{O}_P(V)$ for every i, so $q = \sum_{i=1}^n \frac{a_i}{b} p_i$, i.e. I is finitely generated by $p_1, \dots, p_n$. □

Proposition 2.1.8. *Let R be an integral domain that is not a field. The following are equivalent:*

1. *R is a Noetherian local ring, whose unique maximal ideal is principal.*
2. *There is an irreducible $t \in R$ having the following property: for every nonzero $z \in R$, there is a unique representetaion $z = ut^n$ where $u \in R$ is a unit and $n \in \mathbb{Z}_+$ a nonnegative integer.*

*A ring satisfying these conditions is called a **discrete valuation ring (DVR)**. The element t is called a **uniformizing parameter**.*

Proof. Suppose that condition (1) holds. Let (t) be the maximal ideal generated by $t \in R$. The element t must be irreducible; otherwise an irreducible factor of t would produce a strictly larger ideal. Any unit u of R clearly has a representation $u = ut^0$, so let x be a non-unit. Beacuse R is local, by Lemma 2.1.5 the maximal ideal contains exactly the non-units, so $x \in (t)$ i.e. $x = x_1 t$ for some $x_1 \in R$. If x_1 is a unit, we have found a representation as in (2). Otherwise $x_1 = x_2 t$ for some $x_2 \in R$, whereby $(x_1) \subseteq (x_2)$. Continuing this pattern, we get an ascending chain of ideals $(x_1) \subseteq (x_2) \subseteq (x_3) \subseteq \dots$.

If some x_n is eventually a unit, we obtain a representation $x = x_n t^n$. Assume on the contrary that this never happens. Now the union $\bigcup_{i \geq 1}(x_i)$ of the ascending chain of ideals is itself an ideal and has finite generators $y_1, \dots, y_m$. Then there must be n large enough so that (x_n) contains all of the y_i, and the increasing union does not grow thereafter. It follows that $(x_n) = (x_{n+1})$ i.e. $x_n = ux_{n+1}$ for a unit u. But now $x_n = utx_n$ whereby $ut = 1$ and t must be a unit, which is a contradiction.

To show uniqueness, let $ut^n = vt^m$ for units u, v and nonnegative integers $n \geq m$. Then $ut^{n-m} = v$ and t^{n-m} must be a unit. But t is not a unit, so this is only possible if $n - m = 0$, i.e. $n = m$ and $u = v$. We have proven the implication (1) $\implies$ (2).

Now suppose that condition (2) holds. It is easily seen that the ideal (t) contains exactly the non-units of R, and hence R is local. It then remains to show that R is Noetherian. Let $I \neq (0)$ be a proper ideal, whereby $I \subseteq (t)$. Then the set

$$\{n \in \mathbb{N} \mid \text{ there exists a unit } u \text{ s.t. } ut^n \in I\}$$

is nonempty and contains the smallest element $m \in \mathbb{N}$. Now for any $x = vt^n \in I$, $n \geq m$, we get $x = vt^{n-m}t^m$. In other words, $x \in (t^m)$ and $I = (t^m)$. Because R and (0) are also principal, R is a PID and in particular Noetherian. Hence condition (2) implies condition (1). $\square$

2.2 Affine plane curves and singularities

Recall that the *degree* of a monomial $X_1^{a_1} \dots X_n^{a_n} \in k[X_1, \dots, X_n]$ is defined to be the sum of exponents $a_1 + \cdots + a_n$, and the degree of a constant is 0. The degree of a polynomial p is the largest of the degrees of its monomials, denoted $\deg(p)$. A polynomial whose monomials all have the same degree m is called a *form of degree* m. For example, $X^4 + XY^3 \in k[X, Y]$ is a form of degree 4. By grouping terms with the same degree, every polynomial p can be written as $p = F_0 + F_1 + \cdots + F_j$, where F_i is a form of degree i.

For $i = 1, \dots, n$, the *derivative* g_{X_i} of a monomial $g = X_1^{a_1} \dots X_n^{a_n}$ is defined as

$$g_{X_i} = a_i X_1^{a_1} \dots X_i^{a_i - 1} \dots X_n^{a_n}.$$

The derivative of a polynomial p is the sum of derivatives of its monomials, and obeys the usual differentiation rules with respect to sums, products and constant multiples of polynomials.

We are ready to introduce and study our main object of interest. An *affine plane curve* is an affine algebraic set in $\mathbb{A}^2$ given by a nonconstant polynomial $F \in k[X, Y]$. Note that $\mathcal{V}(F) = \mathcal{V}(cF)$ for any nonzero constant $c \in k$, so we identify affine plane curves up to constant multiples of their defining polynomials. We will say "plane curve" or simply "curve" for short, speak about "the curve F" instead of "the curve $\mathcal{V}(F)$", and use notation such as $\Gamma(F)$ instead of $\Gamma(\mathcal{V}(F))$. The degree of a curve is the degree of its defining polynomial; in particular a curve of degree 1 is called a *line*.

By Proposition 2.1.4 and Hilbert's Nullstellensatz, $\mathcal{V}(F)$ is a variety if and only if $\mathcal{I}(\mathcal{V}(F)) = \sqrt{(F)}$ is a prime ideal, if and only if F is irreducible. In this case $\Gamma(F), k(F)$ and $\mathcal{O}_P(F)$ are well-defined.

If $F(P) = 0$ for a point $P \in \mathbb{A}^2$, we say that P is a point on the curve F, denoted $P \in F$. Let P be a point on a plane curve $F \in k[X, Y]$. It is called a *simple point of* F if $F_X(P) \neq 0$ or $F_Y(P) \neq 0$ i.e. at least one derivative is nonzero. For a simple point $P = (a, b) \in F$, the equation $F_X(P)(X - a) + F_Y(P)(Y - b) = 0$ defines the *tangent line* to F at P. If a point is not simple, it is called a *singular point* or a *singularity*. Singular points of plane curves are those points without a unique tangent line. A curve without singularities is called a *nonsingular* curve.

We can study the tangent lines of any curve at $P = (0, 0)$ by looking at the lowest degree form of the curve. Specifically: write the curve F as a sum of forms $F = F_m + F_{m+1} + \cdots + F_j$, where $F_m \neq 0$. Then $m = m_P(F)$ is called the *multiplicity of* F at $P = (0, 0)$. If $m = 1$, then at least one of the derivatives $(F_m)_X$ or $(F_m)_Y$ is nonzero at P, so P is a simple point. In this case, F_m is exactly the tangent line through P. In the case where $m > 1$, $(F_m)_X(P) = (F_m)_Y(P) = 0$ and P is singular. It turns out F_m factors into m lines passing through P, which serves to motivate the name *multiplicity*:

Proposition 2.2.1. *If k is algebraically closed, then any form $f \in k[X, Y]$ is a product of lines.*

To show this, we will utilize a way to move f to $k[X]$, factor into linear factors by algebraic closure, and move back to $k[X,Y]$.

If $f \in k[X,Y]$ is a form, define $f_* = f(X,1) \in k[X]$ to be the *dehomogenization* of f with respect to Y. For arbitrary $g = a_0 + a_1X + \dots a_jX^j$, where $a_j \neq 0$, define $g^* = a_0Y^j + a_1Y^{j-1}X + \cdots + a_jX^j$ to be the *homogenization* of g with respect to Y. In particular, g^* is a form of degree j.

Lemma 2.2.2. *Let $g, h \in k[X]$ be arbitrary, and $f \in k[X,Y]$ a nonzero form.*

1. $(gh)^* = g^*h^*$
2. *If Y^r is the highest power of Y that divides f, then $f = Y^r(f_*)^*$*

Proof. 1. If $g = a_0 + a_1X + \cdots + a_nX^n$ and $h = b_0 + b_1X + \cdots + b_mX^m$, then

$$(gh)^* = \left(\sum_{i=0}^{n}\sum_{j=0}^{m} a_ib_jX^{i+j}\right)^* = \sum_{i=0}^{n}\sum_{j=0}^{m} a_ib_jX^{i+j}Y^{m+n-(i+j)}$$
$$= \sum_{i=0}^{n} a_iX^iY^{n-i} \sum_{j=0}^{m} b_jX^jY^{m-j} = g^*h^*$$

2. If f is of degree d, then $f_* \in k[X]$ has degree $d-r$. Further, $(f_*)^* \in k[X,Y]$ is a form of degree $d-r$ and $Y^r(f_*)^*$ a form of degree d. But the powers of X in each term have not changed, so the same must be true for the powers of Y, and hence $f = Y^r(f_*)^*$.

□

The proof of Proposition 2.2.1 now follows quickly.

Proof of Proposition 2.2.1. Let $f \in k[X,Y]$ be a form of degree d and Y^r be the highest power of Y that divides f. Because k is algebraically closed, $f_* \in k[X]$ factors into $d-r$ linear factors $X - a_i$ up to constant multiples. Using Lemma 2.2.2, we get

$$f = Y^r(f_*)^* = Y^r\left(\prod_{i=1}^{d-r}(X-a_i)\right)^* = Y^r\prod_{i=1}^{d-r}(X-a_i)^* = Y^r\prod_{i=1}^{d-r}(X-a_iY).$$

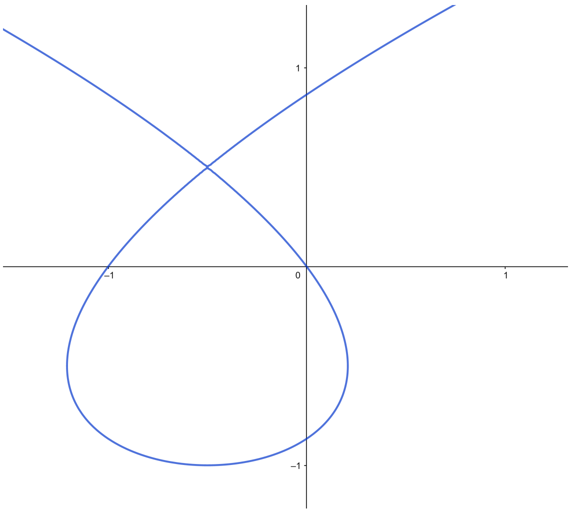
□

Now let $F = F_m + F_{m+1} + \cdots + F_j$ again be a curve with $F_m \neq 0$. By the proposition, write $F_m = \prod_{i=1}^{n} L_i^{r_i}$, where L_i are distinct lines up to constant multiples and $r_1 + \cdots + r_n = m$. The lines L_i are the *tangent lines to* F at P, with *multiplicities* r_i. If $r_i = 1$ for every i, F has m distinct tangents at P, and P is called an *ordinary singular point.*

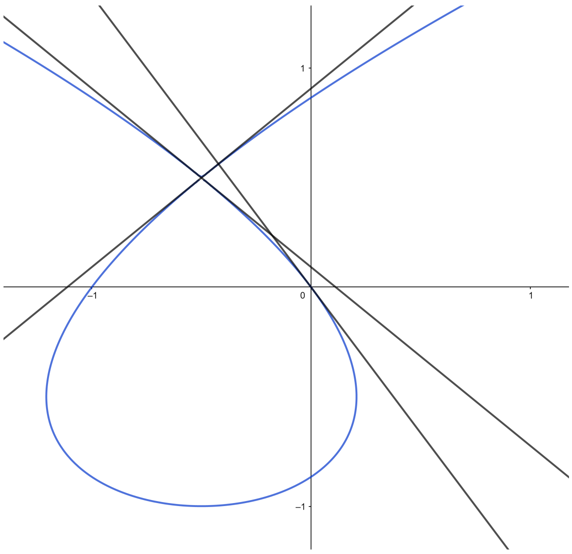
So far we have looked at tangent lines at $P = (0,0)$. For nonzero $P = (a,b) \in F$, let $T : \mathbb{A}^2 \to \mathbb{A}^2, (x,y) \mapsto (x+a, y+b)$ be the translation by P, and $F^T = F(X+$

$a, Y+b)$. We see that T maps the points of F^T to the points of F, and in particular takes $(0,0)$ to P. As before, we can write F^T as a sum of forms $F_m + F_{m+1} + \cdots + F_j$, where $F_m \neq 0$ is of lowest degree. The multiplicity of F at $P = (a,b)$ is defined to be $m_P(F) = m_{(0,0)}(F^T) = m$, and from $F_m = \prod_{i=1}^n L_i^{r_i}$ we get the tangent lines L_i to F^T at $(0,0)$. For $L_i = a_iX + b_iY$, the translations $a_i(X-a) + b_i(Y-b)$ are the tangent lines to F at $P = (a,b)$. Note that $F_X(P) = F^T_X(0,0) = 0$ and $F_Y(P) = F^T_Y(0,0) = 0$ if and only if $m > 1$, so simple points are again exactly those with multiplicity 1.

To wrap up this section, the following example illustrates some tangent lines of a plane algebraic curve.



$X + \frac{3}{4}Y + X^2 - Y^3 = 0$



With tangents at $(0,0)$ *and* $(-\frac{1}{2}, \frac{1}{2})$, *computed below.*

Example 2.2.3. Denote $F = X + \frac{3}{4}Y + X^2 - Y^3$ and $P = (0,0), Q = (-\frac{1}{2}, \frac{1}{2})$. We compute $F_X(P) = 1 \neq 0$ and $F_X(Q) = 1 + 2\cdot(-\frac{1}{2}) = 0$, $F_Y(Q) = \frac{3}{4} - 3\cdot(\frac{1}{2})^2 = 0$. This shows that P is a simple point and Q a singular point, as the image suggests. At the point P, the unique tangent line is given by $X + \frac{3}{4}Y = 0$. To find the tangent lines at Q, we need the above method. Let $T(x,y) = (x - \frac{1}{2}, y + \frac{1}{2})$ be the translation by Q. Then $F^T = X^2 - \frac{3}{2}Y^2 - Y^3$, whose lowest degree form $X^2 - \frac{3}{2}Y^2$ factors into two lines as $\left(X - \sqrt{\frac{3}{2}}Y\right)\left(X + \sqrt{\frac{3}{2}}Y\right)$. Translating back, the lines $X - \sqrt{\frac{3}{2}}Y + \frac{1}{2}\left(1 + \sqrt{\frac{3}{2}}\right) = 0$ and $X + \sqrt{\frac{3}{2}}Y + \frac{1}{2}\left(1 - \sqrt{\frac{3}{2}}\right) = 0$ are the tangents at Q, plotted above.

2.3 Characterizing simple points by local rings

In this section, we will prove two theorems linking the local geometric behaviour of curves (multiplicity, simple or singular) to the properties of their local rings.

Theorem 2.3.1. *Let F be an irreducible curve and $P \in F$. Then P is a simple point of F if and only if $\mathcal{O}_P(F)$ is a discrete valuation ring. In this case, if $L = aX + bY + c$*

is any line through P not tangent to F at P, the image of L in $\mathcal{O}_P(F)$ is a uniformizing parameter for $\mathcal{O}_P(f)$.

Theorem 2.3.2. *Let F be an irreducible curve and $P \in F$. For all sufficiently large $n \in \mathbb{N}$,*

$$m_P(F) = \dim_k \left(\mathfrak{m}_P(F)^n / \mathfrak{m}_P(F)^{n+1}\right)$$

where $\dim_k$ denotes dimension as a k-vector space.

Theorem 2.3.2 will be used in the proof of Theorem 2.3.1, but proved independently afterwards. It requires more preparation, however.

The rough idea for the proof of Theorem 2.3.1 is as follows. For the first implication, to make calculations easier, we show that F can be transformed to a different curve with tangent line Y and non-tangent line X at $(0,0)$, with the local ring isomorphic to that of P of F. For the converse implication, we will compute $m_P(F)$ with the help of Theorem 2.3.2, and use the fact that P is simple if and only if $m_P(F) = 1$.

An *affine change of coordinates* $T : \mathbb{A}^n \to \mathbb{A}^n$ is a bijective linear map followed by a translation. Every such map can be written as $T = (T_1, \dots, T_n)$ where each T_i is a line, i.e. $T_i = a_{i0} + \sum_{j=1}^n a_{ij} X_j$. Every affine change of coordinates has an inverse which is itself an affine change of coordinates. If V is an algebraic set of $\mathbb{A}^n$ generated by $(p_1, \dots, p_m)$, then $V^T := T^{-1}(V)$ is an algebraic set generated by $(p_1 \circ T, \dots, p_m \circ T)$.

Lemma 2.3.3. *Let $P, P' \in \mathbb{A}^2$, let L_1, L_2 be distinct lines through P, and let L_1', L_2' be distinct lines through P'. Then there exists an affine change of coordinates T of $\mathbb{A}^2$ such that $T(P) = P'$, $T(L_1) = L_1'$ and $T(L_2) = L_2'$.*

Proof. First consider the case where $P = P' = (0,0)$. Write $L_1 = a_1 X + b_1 Y, L_1' = a_1' X + b_1' Y$ and similarly for L_2, L_2'. The lines are spanned by the points $Q_1 = (a_1, -b_1), Q_2 = (a_2, -b_2), Q_1' = (a_1', -b_1')$ and $Q_2' = (a_2', -b_2')$. By assumption, the lines are distinct, so Q_1, Q_2 and Q_1', Q_2' are pairwise linearly independent. Then $\{Q_1, Q_2\}$ and $\{Q_1', Q_2'\}$ are bases for $\mathbb{A}^2$, so there exists a unique linear transformation H mapping Q_1 to Q_1' and Q_2 to Q_2'. In particular, H has full rank i.e. is bijective and maps $L_i = \mathrm{span}(Q_i)$ to $L_i' = \mathrm{span}(Q_i')$.

For general P, P', we translate P_1 to $(0,0)$, transform the lines to each other, and translate back out to P_2. The affine change of coordinates

$$T(x,y) = H((x,y) - P_1) + P_2 = H(x,y) - H(P_1) + P_2$$

has the desired property. □

Lemma 2.3.4. *Let T be an affine change of coordinates of $\mathbb{A}^n$, and V a variety. Suppose $Q \in V, P \in V^T$ and $T(P) = Q$. Then the map*

$$\tilde{T} : \mathcal{O}_Q(V) \to \mathcal{O}_P(V^T), \quad \tilde{T}\left(\frac{a}{b}\right) = \frac{a \circ T}{b \circ T}$$

is an isomorphism.

Proof. Composition with T is well-behaved under sums and products. Write $T = (T_1, \dots, T_n)$ and $Y_i = T_i(X_1, \dots, X_n)$ for each $i = 1, \dots, n$. Then for polynomials $f, g \in k[X_1, \dots, X_n]$ we have

$$(f+g) \circ T = (f+g)(Y_1, \dots, Y_n) = f(Y_1, \dots, Y_n) + g(Y_1, \dots, Y_n) = f \circ T + g \circ T$$

and

$$(fg) \circ T = (fg)(Y_1, \dots, Y_n) = f(y_1, \dots, Y_n) g(Y_1, \dots, Y_n) = (f \circ T)(g \circ T).$$

Next we show that $\tilde{T}$ is well-defined. For $g \in \mathcal{I}(V)$ it is clear that $g \circ T \in \mathcal{I}(V^T)$. With $f \in \Gamma(V) = k[X_1, \dots, X_n]/\mathcal{I}(V)$ we have $(f+g) \circ T = f \circ T + g \circ T = f \circ T$, since $g \circ T$ is the zero element of the quotient ring $\Gamma(V^T)$. We see that the map $\Gamma(V) \to \Gamma(V^T) : f \mapsto f \circ T$ does not depend on the choice of representative, so the same can be said for $\tilde{T}$. Further, for any $\frac{a}{b} \in \mathcal{O}_Q(V)$, we have $b(Q) \neq 0$ whereby $(b \circ T)(P) = b(T(P)) = b(Q) \neq 0$ and $\tilde{T} : \mathcal{O}_Q(V) \to \mathcal{O}_P(V^T)$ is well-defined.

By the above properties,

$$\tilde{T}\left(\frac{a}{b} + \frac{c}{d}\right) = \frac{(ad+bc) \circ T}{(bd) \circ T} = \frac{(a \circ T)(d \circ T) + (b \circ T)(c \circ T)}{(b \circ T)(d \circ T)} = \tilde{T}\left(\frac{a}{b}\right) + \tilde{T}\left(\frac{a}{b}\right)$$

and

$$\tilde{T}\left(\frac{a}{b} \cdot \frac{c}{d}\right) = \frac{(ac) \circ T}{(bc) \circ T} = \frac{(a \circ T)(c \circ T)}{(b \circ T)(d \circ T)} = \tilde{T}\left(\frac{a}{b}\right) \cdot \tilde{T}\left(\frac{c}{d}\right),$$

so $\tilde{T}$ is a homomorphism.

Because T is an affine change of coordinates, so is T^{-1} and by the same reasoning as before,

$$\tilde{T}^{-1} : \mathcal{O}_P(V^T) \to \mathcal{O}_Q(V) : \frac{a}{b} \mapsto \frac{a \circ T^{-1}}{b \circ T^{-1}}$$

is a well-defined homomorphism. Then it is easy to see that $\tilde{T}$ and $\tilde{T}^{-1}$ are inverses, so $\tilde{T}$ is bijective and all in all an isomorphism. □

If $G \in k[X, Y]$, we denote by g the residue class of G in $\Gamma(F)$. In particular, x and y are the residues of X and Y. We are ready to prove Theorem 2.3.1:

Proof of Theorem 2.3.1. Let $P \in F$ be simple, L_1 be the unique tangent to F at P and L_2 another line through P not tangent to F. By Lemmas 2.3.3 and 2.3.4, we can take $P = (0,0), L_1 = Y$ and $L_2 = X$. The maximal ideal of $\mathcal{O}_P(F)$ was shown to be

$$\mathfrak{m}_P(F) = \left\{ \frac{a}{b} \in \mathcal{O}_P(F) \mid a(P) = 0 \right\}.$$

Because $P = (0,0)$, the numerators of elements of $\mathfrak{m}_P(F)$ are exactly those without constant terms, i.e. elements of the ideal (x, y). Since $b(P) \neq 0$ by definition of $\mathcal{O}_P(F)$, we see that $\mathfrak{m}_P(F) = (x, y)$. We show that in fact $\mathfrak{m}_P(F) = (x)$. Then, by Proposition 2.1.8, $\mathcal{O}_P(F)$ is a DVR.

We assumed that Y is the tangent to F at $(0,0)$, so Y is the lowest degree form of F and we write $F = Y + W$ with $\deg(W) \geq 2$. Separating terms of W with or without a factor Y yields $F = YG - X^2H$, where $G = 1 + G'$, $\deg(G') \geq 1$, and $H \in k[X]$. But since the residue f of F is zero in $\Gamma(F)$, it follows that $yg = x^2h$. Because G has a constant term, so does every representative of g and hence $g(P) = g(0,0) \neq 0$. Hence we can embed into $\mathcal{O}_P(F)$ and divide by g, which gives $y = x^2hg^{-1} \in (x)$. Thus $\mathfrak{m}_P(F) = (x)$ and $\mathcal{O}_P(F)$ is a discrete valuation ring.

For the converse implication, suppose $\mathcal{O}_P(F)$ is a discrete valuation ring. Then if $t \in \mathcal{O} := \mathcal{O}_P(F)$ is a uniformizing parameter, we have $\mathfrak{m} := \mathfrak{m}_P(F) = (t)$ and $\mathfrak{m}^n = (t^n)$ for all $n \in \mathbb{N}_1$.

By Proposition 2.1.8, we get

$$(t^n) = \{ut^j \mid j \geq n, u \text{ a unit in } \mathcal{O}\}.$$

Then each element $z \in \mathfrak{m}^n/\mathfrak{m}^{n+1} = (t^n)/(t^{n+1})$ is of the form $ut^n + \mathfrak{m}^{n+1}$. Since $u = \frac{a}{b}$ is a unit, it means that $a(P), b(P) \neq 0$. Let $\lambda = \frac{a(P)}{b(P)} \in k$, then

$$u - \lambda = \frac{a - \frac{a(P)}{b(P)}b}{b} \in \mathfrak{m} = (t),$$

because the numerator evaluates to 0 at P. Now $(u - \lambda)t^n \in (t^{n+1}) = \mathfrak{m}^{n+1}$, so

$$ut^n + \mathfrak{m}^{n+1} = (\lambda t^n + (u - \lambda)t^n) + \mathfrak{m}^{n+1} = \lambda t^n + \mathfrak{m}^{n+1}.$$

We see that $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ consists of k-multiples of $t^n + \mathfrak{m}^{n+1}$, so $\dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = 1$ for every $n \geq 1$. Theorem 2.3.2 now implies that $m_P(F) = 1$ i.e. P is a simple point of F. □

The proof of Theorem 2.3.2 will require more preparation, in particular a bit of linear algebra. Recall that a sequence of vector spaces and linear maps

$$V_0 \xrightarrow{\varphi_1} V_1 \xrightarrow{\varphi_2} V_2 \xrightarrow{\varphi_3} \dots \xrightarrow{\varphi_n} V_n$$

is called *exact* if $\ker \varphi_i = \operatorname{im} \varphi_{i-1}$ for each i. A similar notion applies to sequences of groups or rings, and homomorphisms between them.

Lemma 2.3.5. *Let*

$$0 \longrightarrow V' \xrightarrow{\psi} V \xrightarrow{\varphi} V'' \longrightarrow 0$$

be an exact sequence of finite-dimensional vector spaces over k. Then $\dim V = \dim V' + \dim V''$.

Proof. There are unique linear maps $0 \to V'$ and $V'' \to 0$ with image 0 and kernel V'' respectively. By exactness, $\ker \psi = \{0\}$, so ψ is injective and $\dim(\ker \varphi) = \dim(\operatorname{im} \psi) = \dim V'$. On the other hand, $\operatorname{im} \varphi = V''$, so by the rank-nullity theorem, $\dim V = \dim(\ker \varphi) + \dim(\operatorname{im} \varphi) = \dim V' + \dim V''$. □

Lemma 2.3.6. *Let $I = (X, Y) \subset k[X, Y]$ be the ideal generated by X and Y. Then for every $n \in \mathbb{N}_1$,*

$$\dim_k(k[X, Y]/I^n) = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Proof. In the quotient ring $k[X, Y]/I^n$, terms of degree n or more are identified with zero, so we have a spanning set consisting of all monomials of degree less than n. Counting these by degree, we have

$$\begin{aligned}
&\deg 0: && 1\\
&\deg 1: && X, Y\\
&\deg 2: && X^2, XY, Y^2\\
&\dots && \dots\\
&\deg j: && X^iY^{j-i}, i = 0, \dots, j
\end{aligned}$$

i.e. for degree j there are $j + 1$ spanning monomials. But all of these are linearly independent over k and as such form a basis of $k[X, Y]/I^n$. We get

$$\dim_k(k[X, Y]/I^n) = (0 + 1) + (1 + 1) + \cdots + (n - 1 + 1) = 1 + 2 + \cdots + n,$$

as desired. □

Lemma 2.3.7. *Let F be an irreducible curve and $P = (0, 0) \in F$. Let $I = (X, Y) \subset k[X, Y]$ be the ideal generated by X and Y. Then for every $n \geq 1$,*

$$\mathcal{O}_P(F)/\mathfrak{m}_P(F)^n \cong k[X, Y]/(I^n, F).$$

Proof. To make the notation more fluent, write $\mathcal{O}$ and $\mathfrak{m}$ instead of $\mathcal{O}_P(F)$ and $\mathfrak{m}_P(F)$. First note that $\mathfrak{m} = I\mathcal{O}$, because the non-units are exactly those whose numerator vanishes at $P = (0, 0)$. It follows that $\mathfrak{m}^n = (I\mathcal{O})^n = I^n\mathcal{O}$.

For a polynomial $G \in k[X, Y]$ we denote by g its residue in $\Gamma(F)$. Consider the map

$$\rho : k[X, Y] \to \mathcal{O}/I^n\mathcal{O}, \ \rho(G) = \frac{g}{1} + I^n\mathcal{O}.$$

It a composition of three homomorphisms: The quotient map $k[X, Y] \to \Gamma(F)$, the inclusion $\Gamma(F) \to \mathcal{O}$ and the quotient map $\mathcal{O} \to \mathcal{O}/I^n\mathcal{O}$. Thus ρ itself is a homomorphism, which we now show to be surjective. Let $\frac{a}{b} + I^n\mathcal{O} \in \mathcal{O}/I^n\mathcal{O}$. It is in the image of ρ, if it has a representative $\frac{c}{1}$, i.e. $\frac{a}{b} - \frac{c}{1} = \frac{a-bc}{b} \in I^n\mathcal{O}$.

Let $A, B \in k[X, Y]$ be representatives of a and b. We will find $C \in k[X, Y]$ such that $A - BC \in I^n$. Note that $B(P) \neq 0$ by definition of $\mathcal{O}$, so $B = \lambda - B_1$ for some $\lambda \in k \setminus \{0\}$, $B_1 \in I$. Choose $C = \frac{1}{\lambda}(A + AB_1 + AB_1^2 + \cdots + AB_1^{n-1})$, so we obtain a telescoping sum

$$\begin{aligned}
A - BC &= A - (\lambda - B_1) \cdot \frac{1}{\lambda}(A + AB_1 + AB_1^2 + \cdots + AB_1^{n-1})\\
&= A - \frac{\lambda}{\lambda}A + \frac{1}{\lambda}B_1^n = \frac{1}{\lambda}AB_1^n.
\end{aligned}$$

Now $B_1^n \in I^n$, so $\rho(C) = \frac{c}{1} + I^n\mathcal{O} = \frac{a}{b} + I^n\mathcal{O}$ and ρ is surjective.

Finally, $\ker\rho = (I^n, F)$, because the quotient map $k[X,Y] \to \Gamma(F)$ takes I^n to $I^n\mathcal{O}$ and F to 0. From the first isomorphism theorem it then follows $k[X,Y]/(I^n, F) \cong \mathcal{O}/\mathfrak{m}^n$. $\square$

We are ready to prove Theorem 2.3.2. The rough strategy is to find an exact sequence involving the rings $k[X,Y]/I^n$, whose dimension we can calculate exactly.

Proof of Theorem 2.3.2. Again we use the notation $\mathcal{O} = \mathcal{O}_P(F)$ and $\mathfrak{m} = \mathfrak{m}_P(F)$, and write m instead of $m_P(F)$. We have an exact sequence

$$0 \longrightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1} \xrightarrow{i} \mathcal{O}/\mathfrak{m}^{n+1} \xrightarrow{\theta} \mathcal{O}/\mathfrak{m}^n \longrightarrow 0$$

where i is the inclusion map and θ is the map $f + \mathfrak{m}^{n+1} \mapsto f + \mathfrak{m}^n$. It should be noted that θ is well-defined: because $\mathfrak{m}^{n+1} \subset \mathfrak{m}^n$, we have $f + \mathfrak{m}^n = (f+g) + \mathfrak{m}^n$ for any $g \in \mathfrak{m}^{n+1}$ and so the image does not depend on the choice of representative.

We will show that for all $n \geq m$ one has $\dim_k(\mathcal{O}/\mathfrak{m}^n) = nm + s$ for a constant s. In this case, the spaces $\mathcal{O}/\mathfrak{m}^{n+1}$ and $\mathcal{O}/\mathfrak{m}^n$ in the exact sequence are finite-dimensional over k. Then $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ is also finite-dimensional, since i maps it injectively into $\mathcal{O}/\mathfrak{m}^{n+1}$, and by Lemma 2.3.5,

$$\dim(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = \dim(\mathcal{O}/\mathfrak{m}^{n+1}) - \dim(\mathcal{O}/\mathfrak{m}^n) = (n+1)m + s - (nm + s) = m.$$

Again by Lemmas 2.3.3 and 2.3.4, we can assume $P = (0,0)$. Denote $I = (X,Y) \subseteq k[X,Y]$. Now by Lemma 2.3.7, $\mathcal{O}/\mathfrak{m}^n$ is isomorphic to the ring $k[X,Y]/(I^n, F)$. The field k is a subring of both rings, so their k-dimension is the same. Our goal is now to show that $\dim_k(k[X,Y]/(I^n, F)) = nm + s$ for a constant s and all $n \geq m$.

Because $m = m_P(F)$, the lowest degree form of F is of order m. Then if $G \in I^{n-m}$, it follows that $FG \in I^n$. Define the maps

$$\begin{aligned} &\psi : k[X,Y]/I^{n-m} \to k[X,Y]/I^n, && G + I^{n-m} \mapsto FG + I^n \\ &\varphi : k[X,Y]/I^n \to k[X,Y]/(I^n, F), && H + I^n \mapsto H + (I^n, F) \end{aligned}$$

and consider the sequence of k-vector spaces

$$0 \longrightarrow k[X,Y]/I^{n-m} \xrightarrow{\psi} k[X,Y]/I^n \xrightarrow{\varphi} k[X,Y]/(I^n, F) \longrightarrow 0.$$

The map ψ is linear: If $a, b \in k$ and $G, H \in k[X,Y]/I^{n-m}$, then

$$\begin{aligned} \psi(aG + bH) &= F(aG + bH) + I^n = (aFG + I^n) + (bFH + I^n) \\ &= a(FG + I^n) + b(FH + I^n) = a\psi(G) + b\psi(H). \end{aligned}$$

Further, one has $I^n \subseteq (I^n, F)$ so the map φ is a ring homomorphism and thus linear.

Now we see that $\ker\psi = I^{n-m}$, $\operatorname{im}\psi = \ker\varphi = (F+I^n)$ and $\operatorname{im}\varphi = k[X,Y]/(I^n, F)$, so the sequence above is exact. Then by Lemmas 2.3.5 and 2.3.6,

$$\begin{aligned}&\dim_k(k[X,Y]/(I^n,F)) = \dim_k(k[X,Y]/I^n) - \dim_k(k[X,Y]/I^{n-m})\\ &= \frac{n(n+1)}{2} - \frac{(n-m)(n-m+1)}{2} = nm - \frac{m(m-1)}{2}\end{aligned}$$

where $-\frac{m(m-1)}{2}$ is a constant, so we are done. $\square$

We conclude this section with an example. Let $f = X^3 - Y^2$ and $P = (0,0)$. Theorem 2.3.1 now says that $\mathcal{O}_P(f)$ is not a discrete valuation ring. This can be verified in another way.

Every DVR R with $D = \operatorname{Frac}(R)$ has the following property: for all nonzero $a \in D$, either $a \in R$ or $\frac{1}{a} \in R$. If t is a uniformizing parameter of R, then $a = \frac{ut^n}{wt^m} = \frac{u}{w}t^{n-m}$. Since both $\frac{u}{w}$ and $\frac{w}{u}$ are units in R and one of $n-m$ and $m-n$ is nonnegative, indeed either a or $\frac{1}{a} \in R$. More generally, a ring with this property is called a **valuation ring**.

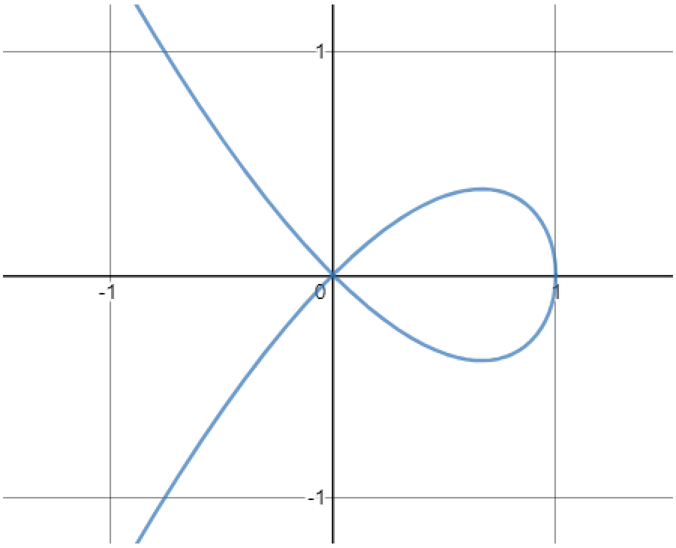
Now with f as above, since we have $\Gamma(f) \subset \mathcal{O}_P(f) \subset k(f) = \operatorname{Frac}(\Gamma(f))$ it follows that $\operatorname{Frac}(\mathcal{O}_P(f)) = k(f)$. We see that $\frac{Y}{X} \in k(f)$ is nonzero, but neither $\frac{Y}{X}$ nor $\frac{X}{Y}$ is in $\mathcal{O}_P(f)$. In other words, $\mathcal{O}_P(f)$ cannot be a DVR, as expected. In fact, since the relation $Y^2 = X^3$ holds on the curve f, we have $\left(\frac{Y}{X}\right)^2 = \frac{X^3}{X^2} = X$ and the rational function $\frac{Y}{X}$ behaves like $\sqrt{X}$ on f. In the complex case, $\frac{Y}{X}$ has the limit 0 as (X,Y) approaches the origin along f. We see that at a singular point, the local ring does not capture all of the well-behaved rational functions.

3 Puiseux expansions

The contents of this chapter are largely based on sources [4] and [8].

3.1 Formal power series

Consider the irreducible plane curve $f(X,Y) = X^3 - X^2 + Y^2$ over $\mathbb{C}$.



Near the origin, it consists of two local branches, which we would like to describe analytically. In this case it is easy: we may solve for Y to get $Y^2 = -X^3 + X^2 = X^2(1-X)$ i.e. $Y = \pm X\sqrt{1-X}$. This yields two parametrizations $t \mapsto (t, t\sqrt{1-t})$ and $t \mapsto (t, -\sqrt{1-t})$ which, when plotted out, do correspond to the branches in the image above. Note that $\sqrt{1-X}$ is analytic for $|X| < 1$ with Maclaurin series $1 - \frac{X}{2} - \frac{X^2}{8} - \frac{X^3}{16} - \frac{5X^4}{128} - \dots$. We are no longer dealing with polynomials, but allowing for power series we can in many cases, even for much more complicated polynomials, give an explicit local parametrization using the so-called *Puiseux expansion*, which will be detailed in this chapter.

We begin by formalizing the notion of power series, so that we can consider curves over not just the complex numbers. Let $m = (m_1, \dots, m_n) \in \mathbb{N}^n$ be a multi-index and $X = (X_1, \dots, X_n)$. We set $|m| = m_1 + \dots + m_n$ and $X^m = X_1^{m_1} \cdot \dots \cdot X_n^{m_n}$. If k is a commutative ring and $a_m \in k$ for every multi-index $m \in \mathbb{N}^n$, then

$$f = \sum_{m \in \mathbb{N}^n} a_m X^m$$

is called a *formal power series of* k. For $d \in \mathbb{N}$, let

$$f_{(d)} = \sum_{|m|=d} a_m X^m \in k[X_1, \dots, X_n]$$

be the *homogeneous part of degree d*. For two formal power series f and g, set

$$f+g=\sum_{d=0}^{\infty}(f_{(d)}+g_{(d)}) \quad \text{and} \quad f\cdot g=\sum_{d=0}^{\infty}\left(\sum_{i+j=d}\left(f_{(i)}g_{(j)}\right)\right).$$

These operations give a ring structure to the set of formal power series. We denote by $k[[X_1,\dots,X_n]]$ the *ring of formal power series* in n variables over k. In particular, for $f\in k[X_1,\dots,X_n]$ we set $a_m=0$ for all $|m|>\deg(f)$. Then f becomes a power series in a natural way, and $k[[X_1,\dots,X_n]]$ is a ring extension of $k[X_1,\dots,X_n]$.

Unlike polynomials, power series in general do not have a degree. Instead, we define

$$\operatorname{ord}(f)=\begin{cases}\min\{d : f_{(d)}\neq 0\} & ,f\neq 0\\ \infty & ,f=0\end{cases}$$

as the degree of the lowest-order term. From the definitions above, we immediately get

$$\begin{aligned}\operatorname{ord}(f+g)&\geq \min\{\operatorname{ord}(f),\operatorname{ord}(g)\},\text{ and}\\ \operatorname{ord}(f\cdot g)&\geq \operatorname{ord}(f)+\operatorname{ord}(g)\end{aligned}$$

for all $f,g\in k[[X_1,\dots,X_n]]$. If k is an integral domain, the second inequality becomes an equality, and $k[[X_1,\dots,X_n]]$ is also an integral domain.

Proposition 3.1.1. *Let $f\in k[[X_1,\dots,X_n]]$. Then f is a unit if and only if the constant term $a_{0\dots0}$ is a unit in k.*

Proof. Necessity: If $fg=1$, then the constant terms of f and g multiply to 1 and the rest vanish. Hence $a_{0\dots0}$ is a unit.

Sufficiency: Let the constant term of f be a unit. By multiplying by the inverse, we can without loss of generality take $a_{0\dots0}=1$. Define

$$\begin{aligned}g&=1-f,\\ h&=1+g+g^2+g^3+\dots\end{aligned}$$

Note that h is well-defined: Because $\operatorname{ord} g\geq 1$, we get $\operatorname{ord} g^m\to\infty$ as $m\to\infty$, and hence terms of each degree appear only finitely many times in the sum. We have constructed an inverse:

$$fh=(1-g)(1+g+g^2+\dots)=1.$$

□

3.2 Newton-Puiseux algorithm

In this section we present an algorithm, often known as the Newton-Puiseux algorithm, which computes Puiseux expansions. Later on, in Theorem 3.2.1, we will prove that these expansions really are the local branches of the input curve.

First, it bears repeating the concept of *characteristic*.

Let R be a ring and denote by 1_R and 0_R the multiplicative and additive identities respectively. The *characteristic* of R is the least number of times 1_R must be added to obtain 0_R; if adding terms 1_R never yields 0_R, the ring R has characteristic 0. This definition naturally applies to fields as well. For example, the finite field $\mathbb{F}_p$ of order a prime number p has characteristic p, while $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ have characteristic 0. In characteristic 0, none of the terms in a binomial expansion will vanish, which as we shall see, will be important in the proof of Theorem 3.2.1.

Let k be an algebraically closed field of characteristic 0, such as the complex numbers. Let $f \in k[[X, Y]]$ be a non-unit not divisible by X. The Newton–Puiseux algorithm outputs a sequence of coefficients $(c_n)_{n\geq 1}$ and a sequence of rational numbers $(\delta_n)_{n\geq 0}$. These are used to form a power series $Y = \varphi(X)$ with rational exponents.

Step-by-step, we proceed as follows:

- Set $f_0 = f$, $X_0 = X$ and $Y_0 = Y$
- Repeat the following steps, starting at $n = 0$ and incrementing n by one after each iteration:

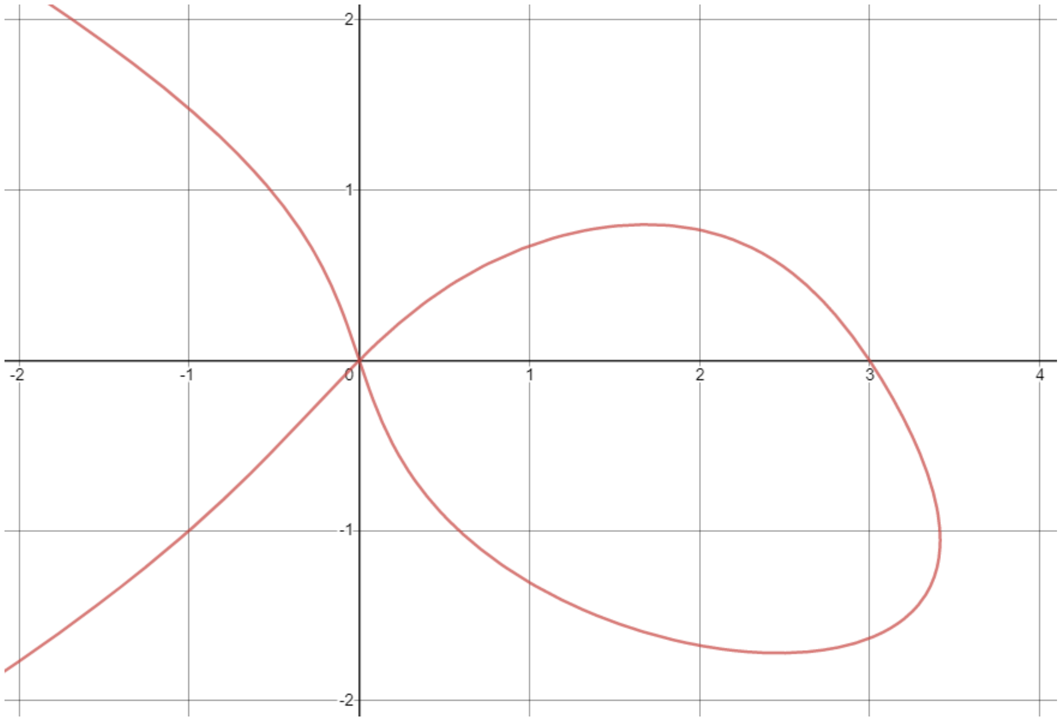
  1. Denote $f_n = \sum_{i,j\geq 0} a_{ij} X_n^i Y_n^j$, where $a_{ij} \in k$ for all i, j.
  2. Let $r_n = \operatorname{ord}(f_n(0, Y_n))$
  3. Compute
  $$\delta_n = \min\left\{ \frac{i}{r_n - j} \mid j < r_0 \text{ and } a_{ij} \neq 0 \right\},$$
  where $\min \emptyset = \infty$.
  4. - If $\delta_n = \infty$, set $c_m = 0$ for all $m > n$ and terminate the algorithm.
     - Otherwise, write
     $$L_{\delta_n}(X_n, Y_n) = \sum_{i+\delta_n j = \delta_n r_n} a_{ij} X_n^i Y_n^j$$
     and choose a nonzero $c_{n+1} \in k$ such that
     $$L_{\delta_n}(1, c_{n+1}) = \sum_{i+\delta_n j=\delta_n r_n} a_{ij} c_{n+1}^j = 0.$$
  5. Write δ_n in reduced form as p_n/q_n.
  Set $X_n = X_{n+1}^{q_n}$ and $Y_n = X_{n+1}^{p_n}(Y_n + c_{n+1})$. Factor f_n as
  $$f_n(X_n, Y_n) = X_{n+1}^{r_n p_n} H(X_{n+1}, Y_{n+1})$$
  and set $f_{n+1} = H$.

The previous steps generate two sequences (c_n) and $(\delta_n) = (p_n/q_n)$. The Puiseux expansion of f is then

$$Y = c_1 X^{\delta_0} + c_2 X^{\delta_0 + \frac{\delta_1}{q_0}} + c_3 X^{\delta_0 + \frac{\delta_1}{q_0} + \frac{\delta_2}{q_0 q_1}} + c_4 X^{\delta_0 + \frac{\delta_1}{q_0} + \frac{\delta_2}{q_0 q_1} + \frac{\delta_3}{q_0 q_1 q_2}} + \dots$$

Let us look at an example of the Newton-Puiseux algorithm, before moving on to closer analysis. Let

$$f = Y^4 + X^3 - 3X^2 + 2XY + Y^2.$$



$Y^4 + X^3 - 3X^2 + 2XY + Y^2 = 0$

This curve has an ordinary singular point at the origin and we would like to find explicit parametrizations for its two branches. Unlike our example at the beginning of this section, we can not immediately take roots to solve for Y. Instead, let us compute a few Puiseux expansion terms as an approximation.

We have $r_0 = 2$, since Y^2 is the lowest pure Y-term, and compute

$$\delta_0 = \min\left\{ \frac{i}{r_0 - j} \mid j < r_0 \text{ and } a_{ij} \neq 0 \right\}.$$

Now $\delta_0 = 1$, since the minimum is reached by both the terms $-3X^2$ and $2XY$. Hence $p_0 = q_0 = 1$, and

$$L_{\delta_0} = \sum_{i+j=2} a_{ij} X^i Y^j = Y^2 + 2XY - 3X^2.$$

Next, $L_{\delta_0}(1,Y) = Y^2 + 2Y - 3$, which yields $c_1 = 1$ or $c_1 = -3$. At this point our path splits; let us first consider the case $c_1 = 1$. Set

$$X = X_1^{q_0} = X_1,\ Y = X_1^{p_0}(Y_1 + c_1) = X_1(Y_1 + 1).$$

Then,

$$\begin{aligned} f &= X_1^4(Y_1+1)^4 + X_1^3 - 3X_1^2 + 2X_1^2(Y_1+1) + X_1^2(Y_1+1)^2 \\ &= X_1^2\left(X_1^2Y_1^4 + 4X_1^2Y_1^3 + 6X_1^2Y_1^2 + 4X_1^2Y_1 + X_1^2 + Y_1^2 + X_1 + 4Y_1\right). \end{aligned}$$

Because $X_1^{r_0p_0} = X_1^2$, the other factor within brackets is our f_1.

Next, $r_1 = 1$ and $\delta_1 = p_1 = q_1 = 1$. Since $L_{\delta_1} = X_1 + 4Y_1$, our only choice of c_2 is $-\frac{1}{4}$. It follows that

$$\begin{aligned} f_2 = X_2^5Y_2^4 - X_2^5Y_2^3 + \frac{3}{8}X_2^5Y_2^2 - \frac{1}{16}X_2^5Y_2 + \frac{1}{256}X_2^5 \\ + 4X_2^4Y_2^3 - 3X_2^4Y_2^2 + \frac{3}{4}X_2^4Y_2 - \frac{1}{16}X_2^4 + 6X_2^3Y_2^2 - 3X_2^3Y_2 \\ + \frac{3}{8}X_2^3 + 4X_2^2Y_2 - X_2^2 + X_2Y_2^2 - \frac{1}{2}X_2Y_2 + \frac{17}{16}X_2 + 4Y_2 \end{aligned}$$

and hence $r_2 = 1$, $\delta_2 = p_2 = q_2 = 1$ and $c_3 = -\frac{17}{64}$. At this point the polynomials become very hard to compute by hand. Lettinge SageMath handle large polynomials for us, we find $r_3 = \delta_3 = p_3 = q_3 = 1$, $c_4 = \frac{111}{512}$ and $r_4 = \delta_4 = p_4 = q_4 = 1$, $c_5 = \frac{2971}{16384}$. The first few terms of

$$Y = c_1X^{\delta_0} + c_2X^{\delta_0 + \frac{\delta_1}{q_0}} + c_3X^{\delta_0 + \frac{\delta_1}{q_0} + \frac{\delta_2}{q_0q_1}} + \dots$$

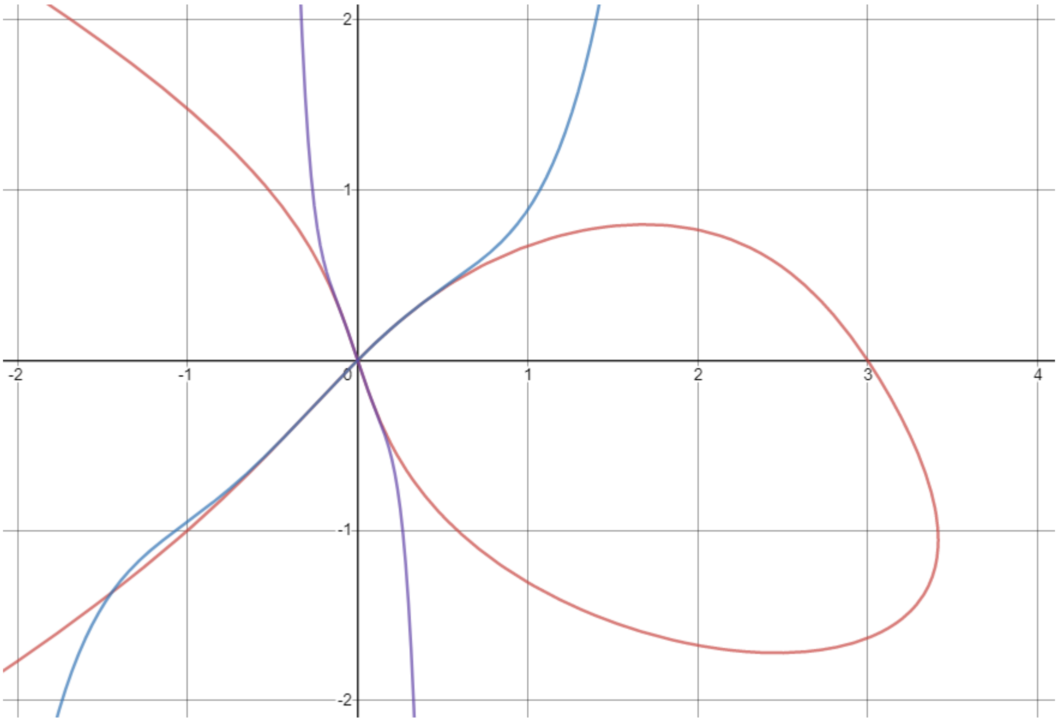
gives us the approximation

$$Y \approx X - \frac{1}{4}X^2 - \frac{17}{64}X^3 + \frac{111}{512}X^4 + \frac{2971}{16384}X^5$$

near the origin.

Now let us consider the case $c_1 = -3$. Omitting the computations here, we find $\delta_i = p_i = q_i$ for $i = 2,3,4$ and $c_2 = \frac{1}{4}$, $c_3 = \frac{1297}{64}$, $c_4 = -\frac{2159}{512}$, $c_5 = -\frac{7277464}{16384}$. Our approximation near the origin is

$$Y \approx -3X + \frac{1}{4}X^2 + \frac{1297}{64}X^3 - \frac{2159}{512}X^4 - \frac{7277464}{16384}X^5.$$



Approximations corresponding to $c_1 = 1$ (increasing curve) and $c_1 = -3$ (decreasing curve) near the origin.

Next, we shall prove that the Newton-Puiseux algorithm has well-defined steps, and that the points given by the Puiseux expansion do indeed lie on the curve.

Theorem 3.2.1 (Newton-Puiseux algorithm)**.** *Let k be an algebraically closed field of characteristic 0, $f \in k[[X,Y]]$ a non-unit such that X does not divide f. Then there exists a natural number $m \geq 1$ and a series $\varphi \in k[[T]]$ such that $\varphi(0) = 0$ and*

$$f(T^m, \varphi(T)) = 0.$$

Proof. Write $f = \sum_{i,j\geq 0} a_{ij} X^i Y^j$, where $a_{ij} \in k$ for all i, j. Let

$$\operatorname{ord}(f(0,Y)) = \min\{j \mid a_{0j} \neq 0\}.$$

Because X does not divide f, this number is finite. We write $r_0 = \operatorname{ord}(f(0,Y)) \geq \operatorname{ord}(f)$. Define

$$\delta_0 = \min\left\{\frac{i}{r_0 - j} \mid j < r_0 \text{ and } a_{ij} \neq 0\right\}$$

where we take $\min \emptyset = \infty$. Now $\delta_0 = \infty$ if and only if $f = a_{0r_0} Y^{r_0} +$ higher terms, or equivalently $f = uY^{r_0}$ where u is a unit in $k[[X,Y]]$.

Suppose $\delta_0 < \infty$. Then for all i, j with $a_{ij} \neq 0$, we have either $j < r_0$ or $j \geq r_0$. In the first case, rearranging $\frac{i}{r_0 - j} \geq \delta_0$ gives $i + \delta_0 j \geq \delta_0 r_0$. But this also holds true in the second case, so we rewrite

$$f = \sum_{i+\delta_0 j \geq \delta_0 r_0} a_{ij} X^i Y^j.$$

Here $a_{0r_0} \neq 0$, and because $\delta_0 < \infty$, the form

$$L_{\delta_0}(X,Y) = \sum_{i+\delta_0 j = \delta_0 r_0} a_{ij} X^i Y^j$$

must have at least two non-zero terms. In particular, $L_{\delta_0}(1,Y) \in k[Y]$ has at least two terms of different degree, so by algebraic closure of k there exists $0 \neq c_1 \in k$ such that

$$L_{\delta_0}(1,c_1) = \sum_{i+\delta_0 j = \delta_0 r_0} a_{ij} c_1^j = 0.$$

We write $\delta_0 = \frac{p_0}{q_0}$ in reduced form and define the variables X_1 and Y_1 via transformations

$$X = X_1^{q_0} \text{ and } Y = X_1^{p_0}(Y_1 + c_1).$$

Since $i + \delta_0 j \geq \delta_0 r_0$ if and only if $q_0 i + p_0 j \geq p_0 r_0$, a direct substitution yields

$$L_{\delta_0}(X,Y) = \sum_{q_0 i + p_0 j = p_0 r_0} a_{ij} X_1^{q_0 i + p_0 j}(Y + c_1)^j = X_1^{r_0 p_0} \sum_{q_0 i + p_0 j = p_0 r_0} a_{ij}(Y + c_1)^j$$

and for terms with $q_0 i + p_0 j \geq p_0 r_0 + 1$, there is a factor X_1 left over when factoring out $X_1^{p_0 r_0}$. We get

$$f = X_1^{r_0 p_0} f_1(X_1, Y_1),$$

where

$$f_1(X_1, Y_1) = \sum_{i+\delta_0 j = \delta_0 r_0} a_{ij}(c_1 + Y_1)^j + X_1 H(X_1, Y_1)$$

for some $H \in k[[X,Y]]$. Note that $f_1(0,0) = L_{\delta_0}(1,c_1) = 0$. Then f_1 is not a unit, and X_1 does not divide f_1. As before, define $r_1 = \operatorname{ord}(f_1(0,Y_1))$. Now $r_1 \leq r_0$ (because in the sum we must have $j \leq r_0$), and we write

$$\begin{aligned}
f_1 &= \sum_{i,j} a_{1,ij} X_1^i Y_1^j, \\
\delta_1 &= \min\left\{ \frac{i}{r_1 - j} \mid j < r_1 \text{ and } a_{1,ij} \neq 0 \right\}.
\end{aligned}$$

If δ_1 is finite, write $\delta_1 = \frac{p_1}{q_1}$ in reduced form. Then we can choose $c_2 \in k$ and define X_2, Y_2 and f_2 by the same steps as before. This yields a sequence of transformations

$$\begin{aligned}
X &= X_1^{q_0}, & Y &= X_1^{p_0}(Y_1 + c_1) \\
X_1 &= X_2^{q_1}, & Y_1 &= X_2^{p_1}(Y_2 + c_2)
\end{aligned}$$

and so on. If we have $\delta_n = \infty$ for some $n \in \mathbb{N}$, then the process terminates; this is because $Y_n^{r_n}$ divides f_n, and hence $Y_n = 0$ is a solution to $f_n(X_n, Y_n) = 0$. Otherwise

$\delta_n < \infty$ for all n and the sequence is infinite. Allowing fractional powers and setting $X_0 = X$ and $Y_0 = Y$, for every n we have that

$$X_n^{\delta_n} = X_{n+1}^{q_n\delta_n} = X_{n+1}^{p_n}$$

yields

$$Y_n = c_{n+1}X_n^{\delta_n} + Y_{n+1}X_n^{\delta_n}.$$

Using these transformations, we can write Y as a fractional power series of X:

$$\begin{aligned} Y &= c_1X^{\delta_0} + Y_1X^{\delta_0} \\ &= c_1X^{\delta_0} + c_2X^{\delta_0+\frac{\delta_1}{q_0}} + Y_2X^{\delta_0+\frac{\delta_1}{q_0}} \\ &= c_1X^{\delta_0} + c_2X^{\delta_0+\frac{\delta_1}{q_0}} + c_3X^{\delta_0+\frac{\delta_1}{q_0}+\frac{\delta_2}{q_0q_1}} + Y_3X^{\delta_0+\frac{\delta_1}{q_0}+\frac{\delta_2}{q_0q_1}} + \dots \end{aligned}$$

If the process terminates early, $Y_n = 0$ for some n yields a finite fractional series. In the case of an infinite series, we wish to show that the exponents of this expansion have bounded denominator (when written in recuded form). We show that there exists $N \in \mathbb{N}$ such that $\delta_n \in \mathbb{N}$ for all $n \geq N$. We have seen that $r_{n+1} \leq r_n$ for all n, and that r_n are always positive. It follows that for some N, $r_n = r_{n+1}$ for all $n \geq N$. For such n, define

$$g(T) = f_{n+1}(0,T) = \sum_{i+\delta_n j = \delta_n r_n} a_{ij}(c_1 + T)^j,$$

which has degree r_n. Further, we get $\operatorname{ord}(g(T)) = \operatorname{ord}(f_{n+1}(0,T)) = r_{n+1} = r_n$, whereby $g(T) = a_{0r_n}T^{r_n}$. We see that

$$g(T-a) = \sum_{i+\delta_n j = \delta_n r_n} a_{ij}T^j = a_{0r_n}(T-c_n)^{r_n}.$$

Expanding the right hand side by the binomial theorem, the term of power $r_n - 1$ must be nonzero, because k has characteristic 0. On the left hand side, we get $a_{i,r_n-1} \neq 0$, where $i + \delta_n(r_n - 1) = \delta_n r_n$. It follows that $\delta_n \in \mathbb{N}$.

Let us return to the expansion

$$Y = c_1X^{\delta_0} + c_2X^{\delta_0+\frac{\delta_1}{q_0}} + c_3X^{\delta_0+\frac{\delta_1}{q_0}+\frac{\delta_2}{q_0q_1}} + \dots$$

Let $N \in \mathbb{N}$ such that $\delta_n \in \mathbb{N}$ (and hence $q_n = 1$) for all $n > N$. Set $m = q_0q_1 \dots q_N$. Then we can write

$$Y = \varphi(X^{\frac{1}{m}}), \text{ for a series } \varphi(T) = \sum_{i=1}^{\infty} b_iT^i.$$

We have $\varphi(0) = 0$, as required. It remains to show that

$$f(T^m, \varphi(T)) = 0 \text{ in } k[[T]].$$

By our construction in the iterative step, we get

$$X = X_1^{q_0} = X_2^{q_0 q_1} = \cdots = X_N^{q_0 \cdots q_N} = X_j^m, \quad j > N.$$

Hence we can set $X = T^m$ and $X_i = T^{q_i \cdots q_N}$ for $i \leq N$, $X_i = T$ for $i > N$. Because $f_i = X_{i+1}^{r_i p_i} f_{i+1}$, it follows that f is divisible by

$$X_1^{r_0 p_0} X_2^{r_1 p_1} \ldots X_{i+1}^{r_i p_i}$$

and substituting in T, f is divisible by T^r, where

$$r = r_0 p_0 q_1 \ldots q_N + r_1 p_1 q_2 \ldots q_N + \cdots + r_{N-1} p_{N-1} q_N + \sum_{j=N}^{i} r_j p_j.$$

Now $r_j, p_j, q_j \geq 1$, so this exponent grows arbitrarily large as $i \to \infty$. Because $f(T^m, \varphi(T))$ is divisible by arbitrarily large powers of T, it follows that $f(T^m, \varphi(T)) = 0$. □

It is worth looking at a simple case where the algorithm terminates early. Consider

$$f = X^2 + Y^2 - 2XY - X.$$

We have $r_0 = 2$, $\delta_0 = \frac{1}{2}$, $L_{\delta_0} = Y^2 - X$, which yields $c_1 = 1$ or $c_1 = -1$.

In the case $c_1 = 1$, we get $f_1 = X_1^2 - 2X_1Y_1 + Y_1^2 - 2X_1 + 2Y_1$, $\delta_1 = c_2 = 1$ and $f_2 = X_2Y_2^2 + 2Y_2$. At this point set $Y_2 = 0$ and get a solution $Y = c_1 X^{\delta_0} + c_2 X^{\delta_0 + \frac{\delta_1}{q_0}} = X^{\frac{1}{2}} + X$. The case $c_1 = -1$ quickly yields $Y = -X^{\frac{1}{2}} + X$ through near identical steps. In this specific case, we may also solve for Y through elementary means to confirm the results: setting $f = 0$ gives $(Y - X)^2 = X$, and taking roots and rearranging gives solutions $Y = X \pm X^{\frac{1}{2}}$, as expected.

The algorithm yields a local parametrization of f around the origin. Should we wish to compute Puiseux series around a different point instead, we can proceed as we did when computing tangents at the end of Section 2.2. Specifically, let $P = (a, b) \in f$ and T be the translation $T : (x, y) \mapsto (x + a, y + b)$. Then we can apply the previous algorithm to $f^T = f(X + a, Y + b)$ (assuming it is not divisible by X) and translate the resulting series back by P.

There is a geometric interpretation of one of the steps in the algorithm. Define the *carrier* of f as

$$\operatorname{carr}(f) = \left\{(i, j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\right\}.$$

We can plot the points of $\operatorname{carr}(f)$ in positive $\mathbb{R}^2$ and draw the lower convex hull of the points – this results in a number of line segments with non-positive slope. The resulting figure is called the *Newton polygon* of f. Note that by assumption, f has no divisor X or a constant term, so the positive Y-axis contains at least one point of the carrier; the lowest of these is $(0, r_0)$. In the step, where we compute

$$\delta_0 = \min\left\{\frac{i}{r_0 - j} \mid j < r_0 \text{ and } a_{ij} \neq 0\right\},$$

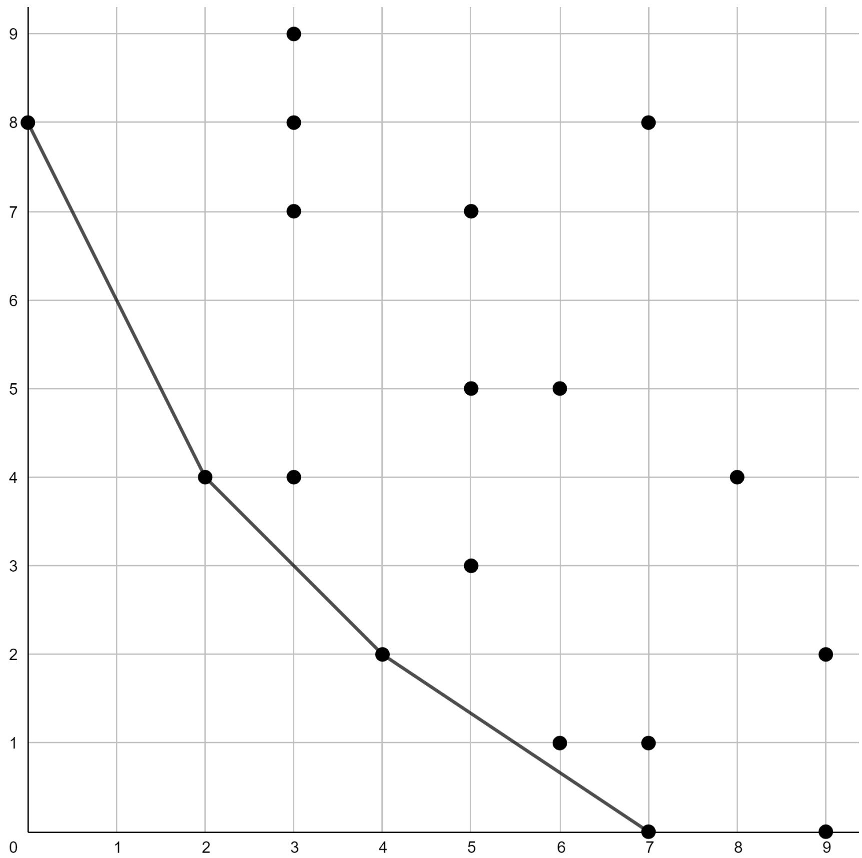


Figure 1: The carrier of f and the Newton polygon

we are in fact computing $-1/m$, where m is the slope of the steepest possible line segment between $(0, r_0)$ and a point of $\mathrm{carr}(f)$ with lower Y-coordinate. In the figure, this line segment lies between $(0, 8)$ and $(2, 4)$. All points of the carrier lie on the right half-plane given by the corresponding line, which justifies the weighted sum representation of f thereafter. It is in fact possible to use other line segments of the Newton polygon to compute Puiseux expansions of f; this results in a different algorithm which is detailed in [6].

It is possible for infinite fields, and even algebraically closed ones, to have positive characteristic. One such example we can easily construct: Let p be a prime number and k be the finite field of order p. Then the field of rational functions $k(X, Y) = \mathrm{Frac}(k[X, Y])$ is infinite, since e.g. the residue classes of $X, X^2, X^3, \dots$ are distinct. But the subfield k contains the multiplicative and additive identities, so $k(X, Y)$ has the same characteristic $p > 0$. It can also be shown that every field has an algebraic closure; for example pages 11-12 of [5] explain how the closure may be constructed. Then the algebraic closure $\bar{k}$ is algebraically closed, but again has characteristic p, since the identities are contained in k. Cutkosky [8] provides a counterexample to the Newton-Puiseux algorithm in characteristic p, which shows that the assumption of characteristic 0 is necessary.

3.3 Finding all branches, and convergence in $\mathbb{C}$

In the Newton-Puiseux algorithm, we must in each step choose a constant c_i. As we have seen, different choices may yield different parametrizations. But we can in fact show that, even if the algorithm never terminates, only finitely many are possible. Again, let $f \in k[[X, Y]]$ fulfill the conditions of Theorem 3.2.1. We will first assume that f is irreducible in $k[[X, Y]]$.

Suppose we have found a solution $f(T^m, \varphi(T)) = 0$, where the natural number m is the smallest possible. Since k is algebraically closed, let r be a primitive m-th root of unity; primitive meaning that $r^n \neq 1$ for $n < m$. Substituting r^jT for T, we get $f(T^m, \varphi(r^jT)) = 0$ for all $0 \leq j \leq m-1$.

In fact, these solutions must be distinct. If $m > 1$, the series $\varphi(T)$ must contain a term of power p relatively prime to m; otherwise if q is a common factor, $\varphi(T^{\frac{1}{q}}) \in k[[T]]$ and $f(T^{\frac{m}{q}}, \varphi(T^{\frac{1}{q}}))$ is a solution contradicting the minimality of m. Now suppose $\varphi(r^iT) = \varphi(r^jT)$ for some $0 \leq i \leq j \leq m-1$. Comparing the terms of power p yields $r^{ip} = r^{jp}$, i.e. $r^{p(j-i)} = 1$. It follows that $m \mid p(j-i)$, but because m and p are relatively prime, we have $m \mid j - i$. Since j and i differ by less than m, we conclude that $j = i$. Hence the solutions for $0 \leq j \leq m-1$ are distinct.

Consider the ring $R_m = k[[X^{\frac{1}{m}}, Y]]$ of which $k[[X, Y]]$ is a subring. Denote $\varphi_j(T) = \varphi(r^jT)$ for each j. Then $Y - \varphi_j(X^{\frac{1}{m}})$ divides f in R_m for each j, and in particular

$$g = \prod_{j=0}^{m-1} \left(Y - \varphi_j(X^{\frac{1}{m}})\right)$$

divides f in R_m.

In fact, g is in $k[[X, Y]]$. Consider the automorphism ψ of R_m induced by $X^{\frac{1}{m}} \mapsto rX^{\frac{1}{m}}$ and $Y \mapsto Y$. Which elements of R_m are fixed by ψ? For some $h \in R_m$, $\psi(h) = h$ if and only if in each term, the power i of $X^{\frac{1}{m}}$ is such that $r^i = 1$. Because r is primitive, i must be a multiple of m (including 0), and hence h contains only integer powers of X, i.e. $h \in k[[X, Y]]$. Hence this subring contains exactly the elements fixed by ψ. But notice that ψ merely permutes the factors of g, so g is also fixed by ψ and hence g divides f in $k[[X, Y]]$. But f is irreducible, so there is a unit $u \in k[[X, Y]]$ such that

$$f = ug = u \prod_{j=0}^{m-1} \left(Y - \varphi_j(X^{\frac{1}{m}})\right).$$

Units have nonzero constant term by Proposition 3.1.1, so u is nonzero at the origin and the branches of f are at least locally determined by g.

We assumed that f is irreducible, but in fact $k[[X, Y]]$ is a unique factorization domain (UFD). In particular, power series over PIDs in any number of variables are UFDs, as proven by P. Samuel [7]. Fields are PIDs, so this holds for $k[[X, Y]]$. Then an arbitrary $f \in k[[X, Y]]$ has only finitely many irreducible factors, and so has only finitely many solutions $Y = \varphi(X^{\frac{1}{m}})$.

So far, what we have obtained are only formal power series solutions to an implicit polynomial equation (or more generally, power series equation). In the case of complex curves, given a convergent input such as a polynomial, we would like the algorithm to return convergent Puiseux expansions as well, at least in a neighbourhood of the origin. This is the case, but a full proof would be lengthy and technical. Brieskorn and Knörrer [1] give a proof of convergence using the theory of Weierstrass polynomials, and we will repeat their main ideas here.

Theorem 3.3.1 (Weierstrass preparation theorem)**.** *Let $f(X,Y) \in \mathbb{C}[[X,Y]]$ be a convergent power series with $\operatorname{ord}(f(0,Y)) = n > 0$. Then there exist convergent power series $u \in \mathbb{C}[[X,Y]]$ and $c_1, \dots, c_n \in \mathbb{C}[[X]]$ such that*

$$f(X,Y) = u(X,Y)\left(Y^n + c_1(X)Y^{n-1} + \cdots + c_n(X)\right),$$

where $c_i(0) = 0$ for each $1 \le i \le n$ and $u(0,0) \ne 0$.

Proof. Cf. Brieskorn and Knörrer [1] □

In the preparation theorem, the power series u converges and is nonzero at the origin. Hence the zeroes of f in a neighbourhood of the origin are given by $Y^n + c_1(X)Y^{n-1} + \cdots + c_n(X)$, which is a polynomial in Y with coefficients in $\mathbb{C}[[X]]$. A polynomial of this form is referred to as a *Weierstrass polynomial.*

The proof of convergence of Puiseux expansions is roughly as follows. In a small enough neighbourhood, f can be assumed to be a Weierstrass polynomial. The existence of a convergent solution $Y = \varphi(X^{\frac{1}{n}})$ to the equation $f(X,Y) = 0$ is shown by the next theorem. This yields n different roots of the Weierstrass polynomial of degree n, and since the Newton-Puiseux algorithm also produces a root, it must coincide with one of the convergent solutions.

For $\varepsilon, \delta > 0$, denote by

$$U_{\varepsilon,\delta} = \{(x,y) \in \mathbb{C}^2 \mid |y| < \varepsilon, |x| < \delta\}$$

the *polydisc* with radii ε and δ.

Theorem 3.3.2. *Let $f(X,Y) \in \mathbb{C}[[X,Y]]$ be an irreducible convergent power series with $\operatorname{ord}(f(0,Y)) = n > 0$. Then there exists $\varepsilon_0 > 0$ such that for every $0 < \varepsilon < \varepsilon_0$, there exists $\delta > 0$ with the following properties:*

Define the sets

$$V = \{(x,y) \in U_{\varepsilon,\delta} \mid f(x,y) = 0\}, \text{ and}$$
$$B = \{z \in \mathbb{C} \mid |z| < \delta^{\frac{1}{n}}\}.$$

Then there exists a convergent power series $\varphi(X) \in \mathbb{C}[[X]]$ such that

$$\pi : B \to \mathbb{C}^2,\ z \mapsto (z^n, \varphi(z)),$$

is holomorphic and onto V, the restriction $\pi : B \setminus \{0\} \to V \setminus \{0\}$ is biholomorphic and $\pi^{-1}(0) = 0$.

Proof. Cf. Brieskorn and Knörrer [1] □

Now let $f \in \mathbb{C}[[X,Y]]$ be convergent and satisfy the conditions of the Newton-Puiseux algorithm (Theorem 3.2.1). By restricting to a small enough neighbourhood of the origin, by the Weierstrass preparation theorem we can without loss of generality assume f to be a Weierstrass polynomial of degree n.

If f is irreducible in $\mathbb{C}[[X,Y]]$, by Theorem 3.3.2 there exists a convergent series $Y = \varphi(X^{\frac{1}{n}})$ which satisfies $f(X,Y) = 0$. Equivalently, this is a root of the Weierstrass polynomial f (which has coefficients in $\mathbb{C}[[X]]$) lying in the ring extension $\mathbb{C}[[X^{\frac{1}{n}}]]$. By similar reasoning as before, we can shift by a primitive n:th root of unity to obtain different solutions. Hence the series $\varphi(e^{\frac{2\pi i m}{n}} X^{\frac{1}{n}})$, for $m = 0, \ldots, n-1$ are also convergent and satisfy $f(X,Y) = 0$. Now the series $\psi(X^{\frac{1}{n}})$ constructed by the Newton-Puiseux algorithm also satisfies $f(X,Y) = 0$, but since a polynomial of degree n has at most n distinct roots, ψ must coincide with one of the previous convergent series.

If f has several irreducible factors, then the Puiseux expansion parametrizes one of the irreducible components, and hence is convergent by the same reasoning as above.

4 Braids of complex plane curve singularities

The complex affine space $\mathbb{C}^2$ is difficult to represent visually, because it consists of four real dimensions. But by intersecting an isolated singularity of a complex plane curve with a small sphere centered around the singularity, one obtains a lower-dimensional object. The topology of these objects is in fact closely related to the Puiseux expansion of the curve. Our goal of this section showing that up to a certain type of equivalence, an irreducible plane curve takes the shape of a so-called *iterated torus knot* around the origin. A full treatment of the subject may be found in Brieskorn's *Plane Algebraic Curves* [1], which much of this chapter is based on.

4.1 The $(p, q)-$torus knot

We begin with a simple special case.

Let $p, q \geq 2$ be relatively prime integers, and consider the complex plane curve

$$f = X^p - Y^q \in \mathbb{C}[X, Y].$$

We will later check that this curve is irreducible. It has a singularity at the origin, and is nonsingular elsewhere. What happens when we intersect the set $\mathcal{V}(f) \in \mathbb{C}^2$ with a sphere around the origin? Specifically, let $\varepsilon > 0$ and define the complex 2-sphere of radius ε as

$$S^2_\varepsilon = \{(z, w) \in \mathbb{C}^2 \mid |z|^2 + |w|^2 = \varepsilon^2\}.$$

For $z = x + iy$, we have $|z|^2 = z\overline{z} = x^2 + y^2$. It will be more convenient to work with polar coordinates. As a reminder, every complex number z can be represented in polar form as $z = re^{i\theta}$, where the real number $r \geq 0$ is the *magnitude* or the *modulus* of z, and $\theta \in \mathbb{R}$ is the *argument*, corresponding to the angle with respect to the real axis in the complex plane. In this case, we simply get $|z| = r$.

Now, writing $X = re^{i\theta}$ and $Y = te^{i\varphi}$, the intersection $\mathcal{V}(f) \cap S^2_\varepsilon$ is determined by the system of equations

$$\begin{cases} r^p e^{ip\theta} = t^q e^{iq\varphi} \\ r^2 + t^2 = \varepsilon^2 \end{cases}$$

Since magnitude is independent of argument, this is further refined as

$$\begin{cases} q\varphi = p\theta + 2\pi n, \;\; n \in \mathbb{Z} \\ r^p = t^q \\ r^2 + t^2 = \varepsilon^2 \end{cases}$$

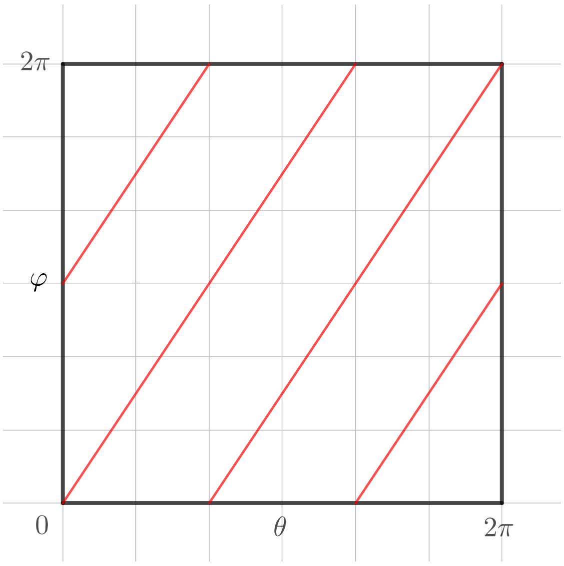
The last two equations have a unique solution. Specifically, since r and t are nonnegative real numbers, we may write $r = t^{\frac{q}{p}}$, whereby $t^{\frac{2p}{q}} + t^2 = \varepsilon^2$. But the left-hand expression is unbounded and strictly increasing from 0, so there is a unique solution $t' > 0$. This in turn uniquely determines $r' = (t')^{\frac{q}{p}} > 0$.

In other words, if we set $\mathbb{S}^1_{r'} = \{z \in \mathbb{C} \mid |z| = r'\}$ and $\mathbb{S}^1_{t'} = \{z \in \mathbb{C} \mid |z| = t'\}$, then the intersection lies on $\mathbb{S}^1_{r'} \times \mathbb{S}^1_{t'}$, which is a topological torus.

The torus can be modelled as a rectangle with opposite sides identified. Then the angle equation

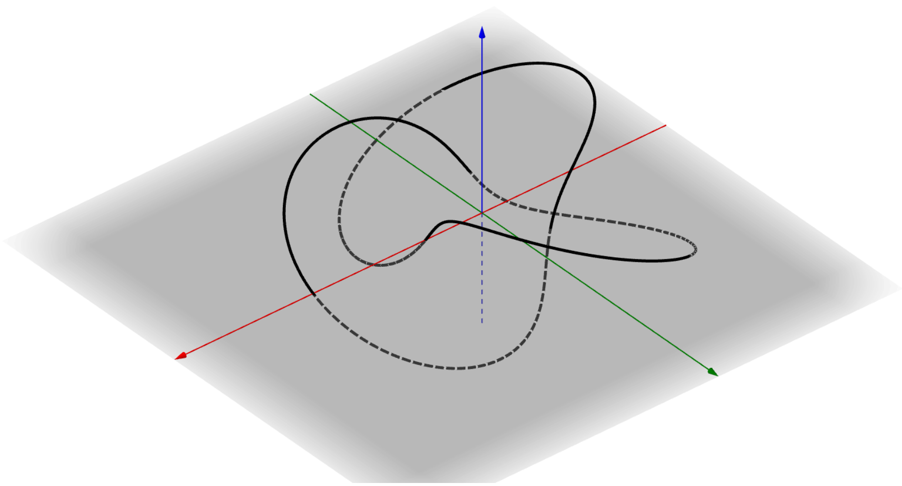
$$\varphi = \frac{p}{q}\theta + 2\pi\frac{n}{q}, \ n \in \mathbb{Z},$$

determines a single line of angle $\frac{p}{q}$ on this rectangle, when wrapping around the edges. This is known as a $(p, q)-$*torus knot*.



The line corresponding to $p = 3, \ q = 2$

The torus surface, along with the knot, may be embedded in $\mathbb{R}^3$. The resulting picture may give some insight into why these curves are called *knots*.

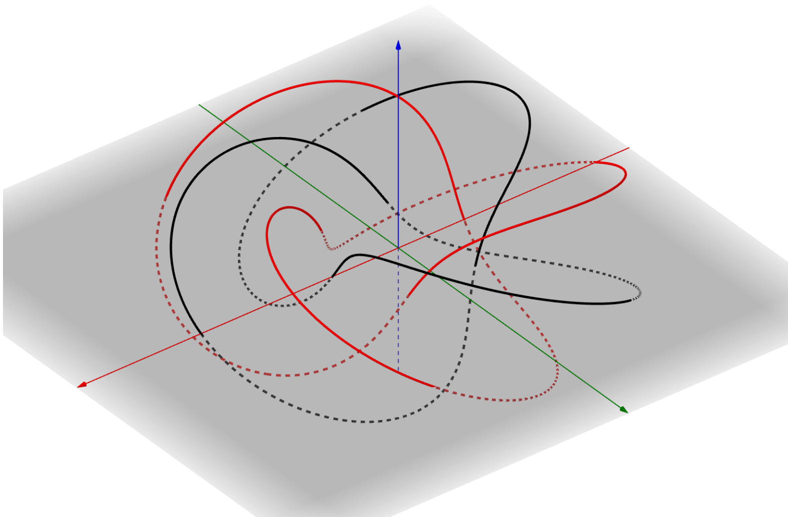


The $(3, 2)$*-torus knot, commonly referred to as the trefoil knot.*

It may be useful to mention what happens in the case where p and q have nontrivial common factors. Suppose $p = p'k$ and $q = q'k$ where p' and q' are relatively prime and $k > 1$. Then the angle equation

$$\varphi = \frac{p'}{q'}\theta + 2\pi \frac{n}{q'k}, \ n \in \mathbb{Z}$$

determines k disjoint lines on the torus of angle $\frac{p'}{q'}$. The result is k separate $(p', q')-$torus knots linked together.



Two linked $(3, 2)$*-knots, corresponding to* $p = 6$, $q = 4$.

This behaviour between single or multiple linked knots depends on the common factors of p and q, which in turn determine the reducibility of the polynomial $f = X^p - Y^q$. Let us quickly verify this.

Proposition 4.1.1. *Let $p, q \geq 1$ be relatively prime. Then the polynomial $X^p - Y^q$ is irreducible in $\mathbb{C}[X, Y]$.*

Proof. Consider the ring homomorphism $\varphi : \mathbb{C}[X, Y] \to \mathbb{C}[t]$ induced by $X \mapsto t^q$ and $Y \mapsto t^p$. Then $\ker \varphi = (X^p - Y^q)$, where the latter is the ideal generated by $X^p - Y^q$. The inclusion "$\supseteq$" is easy to see. In the other direction, for any $g \in \ker \varphi$ we may write $g = h_1(X, Y)(X^p - Y^q) + h_2(X, Y)$ where the degrees of X and Y in each term of h_2 are less than p and q respectively. In other words,

$$h_2(X, Y) = \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} a_{ij} X^i Y^j \mapsto \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} a_{ij} t^{iq+jp} = 0.$$

Because p and q are relatively prime, exponents in the last sum are mutually distinct, and hence the terms are linearly independent over $\mathbb{C}$. Therefore $a_{ij} = 0$ for all i, j, such that $h_2 = 0$ and $g \in (X^p - Y^q)$. Finally, $\operatorname{im} \varphi \cong \mathbb{C}[X, Y]/(X^p - Y^q)$ is a subring of $\mathbb{C}[t]$, which is an integral domain. Then $\operatorname{im}\varphi$ is an integral domain, whereby $(X^p - Y^q)$ is a prime ideal and $X^p - Y^q$ is irreducible. $\square$

In the other case, suppose p and q have a greatest common divisor $k > 1$. Indeed, the polynomial f is now reducible:

$$\begin{aligned} f =& X^p - Y^q = \left(X^{p'}\right)^k - \left(Y^{p'}\right)^k \\ =& \left(X^{p'} - Y^{q'}\right)\left(X^{p'(k-1)} + X^{p'(k-2)}Y^{q'} + \cdots + X^{p'}Y^{q'(k-2)} + Y^{q'(k-1)}\right). \end{aligned}$$

More generally, the so-called *braid* of a reducible curve will consist of the braids of its irreducible components linked together in some manner. Brieskorn [1] investigates this case further; we will instead focus on irreducible curves.

4.2 Puiseux pairs and braids

In the previous special case, the curve $f = X^p - Y^q$ is parametrized entirely by $\psi : \mathbb{C} \to \mathbb{C}^2$, $t \mapsto (t^q, t^p)$. It is straightforward to show that the (p, q)-torus knot obtained by intersection with a sphere is exactly the image of a circle $\mathbb{S}^1 \subset \mathbb{C}$ under ψ. As we have seen, the Puiseux expansion provides a local parametrization of a curve around the origin. In this special case, we have the simple expansion $Y = X^{\frac{p}{q}}$. Naturally, the next step is to look more generally at what happens to small circles under the Puiseux expansion.

Let $f \in \mathbb{C}[X, Y]$ be an irreducible curve with Puiseux expansion $Y = \varphi(X^{\frac{1}{m}})$. For small $\delta > 0$, we define the *braid* of $\varphi(X^{\frac{1}{m}})$ to be its image of the circle $\mathbb{S}^1_\delta$, in other words

$$\left\{\varphi\left((\delta e^{2\pi i t})^{\frac{1}{m}}\right) \mid 0 \le t \le 1\right\}.$$

We first consider $\varphi(X^{\frac{1}{m}})$ informally as a multi-valued function; to each value of X we associate m different points. After we construct the braid of a so-called *standard expansion*, this will be reframed more rigorously, such that the topology of the braids can be studied.

To help us in our study of braids, we introduce a sequence of integer pairs, called the *Puiseux pairs*, which characterize the singularity. The Puiseux pairs essentially correspond to places in the Puiseux expansion where the denominator of the exponent increases, when written in reduced form. As the whole expansion has bounded denominator in the exponents, this will give a finite sequence of integer pairs.

Write the Puiseux expansion of f as

$$Y = \varphi(X^{\frac{1}{m}}) = \sum_{j \in \mathbb{N}} a_j X^{\frac{j}{m}},$$

where $a_j \in \mathbb{C}$. Further, we may assume all exponents in the expansion are at least 1, that is $a_j = 0$ for $j < m$. This assumption helps us avoid cases where the choice of coordinates affects the result; this will be elaborated on later.

For what follows, note that any nonempty subset of the exponents has a smallest element. This is because any nonempty subset of the natural numbers has a smallest element, and the exponents are entirely determined by the numerators, since the denominator m is fixed.

Now proceed as follows. If all exponents are integers, then no Puiseux pairs are defined. Otherwise, there is a smallest exponent q_1 which is not an integer. Denote this exponent by

$$q_1 = \frac{n_1}{m_1}$$

in reduced form, where $n_1 > m_1$. We define (m_1, n_1) to be the *first Puiseux pair* of f. Now if all the succeeding exponents can be written as $\frac{j}{m_1}$ for $j > n_1$, then the sequence of Puiseux pairs terminates. Otherwise, let q_2 be the smallest exponent not of this form. We write

$$q_2 = \frac{q_2 m_1}{m_1} = \frac{n_2}{m_1 m_2},$$

where n_2 and m_2 are relatively prime and $m_2 > 1$, i.e. $\frac{n_2}{m_2}$ is the reduced form of $q_2 m_1$. We define (m_2, n_2) to be the *second Puiseux pair* of f.

Inductively, suppose we have defined the Puiseux pairs $(m_1, n_1), \ldots, (m_i, n_i)$. Let q_{i+1} be the smallest exponent which cannot be written as

$$q = \frac{a}{m_1 \ldots m_i}, \ a \in \mathbb{N}.$$

As before, we write

$$q_{i+1} = \frac{q_{i+1} \cdot m_1 \ldots m_i}{m_1 \ldots m_i} = \frac{n_{i+1}}{m_1 \ldots m_i \cdot m_{i+1}},$$

where n_{i+1} and m_{i+1} are relatively prime, and (m_{i+1}, n_{i+1}) is Puiseux pair number $i+1$ of f. The sequence of Puiseux pairs must be finite, since otherwise the denominators of the exponents in the Puiseux expansion would grow arbitrarily large.

As an example, consider a curve with Puiseux expansion

$$Y = X^{\frac{5}{4}} - X^{\frac{7}{4}} + (2+i)X^{\frac{11}{5}} + 12X^{\frac{33}{10}}.$$

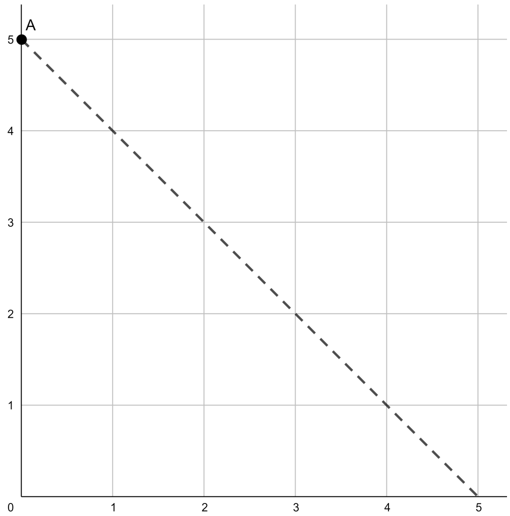
We have $(m_1, n_1) = (4, 5)$. Then $\frac{7}{4}$ can be represented with the same denominator, so we get $q_2 = \frac{11}{5}$ and

$$\frac{n_2}{m_2} = q_2 m_1 = \frac{44}{5}$$

i.e. $(m_2, n_2) = (5, 44)$. Finally, we have $\frac{33}{10} = \frac{66}{20} = \frac{66}{m_1 m_2}$, so no more Puiseux pairs are defined.

Before, we made the additional assumption $q \geq 1$. Via a linear change of coordinates, curves can always be brought to a form whose Puiseux expansion satisfies this additional requirement. Recall the Newton polygon discussed briefly in Section 3.2. The first exponent δ_0 is $-1/m$, where m is the slope of the first line segment on the left. The dotted line in the image corresponds to $\delta_0 = 1$, while lines extending below or above give $\delta_0 < 1$ or $\delta_0 > 1$ respectively. Because the degrees of terms below the line are strictly smaller, the case $\delta_0 \geq 1$ occurs exactly when the carrier of f lies on or above the line, i.e. the lowest degree form of f contains a pure Y-term. This in turn is equivalent to the Y-axis not being a tangent at the origin.

In other words, by taking a linear change of coordinates if necessary, one can always assume exponents are at least 1. In particular, such transformations are homeomorphisms of $\mathbb{C}^2$.



Proposition 4.2.1. *The following properties hold for the Puiseux pairs of any curve (where defined):*

1. $m_1 < n_1$
2. $n_{i-1}m_i < n_i$ *for* $i \geq 2$
3. n_i *and* m_i *are relatively prime for all* i.

Proof. Property 1 comes from the requirement that $q \geq 1$ for all exponents q, and the first Puiseux pair corresponds to the first non-integer exponent. Property 3 is clear by how the pairs are constructed.

Property 2 follows from the inequality

$$\frac{n_{i-1}}{m_1 \dots m_{i-1}} = q_{i-1} < q_i = \frac{n_i}{m_1 \dots m_i}$$

by rearranging and cancelling $m_1 \dots m_{i-1}$. □

Given a finite sequence of integer pairs $(m_1, n_1), \dots (m_i, n_i)$ satisfying the conditions of Proposition 4.2.1, we define the *standard expansion* of the pairs to be

$$\begin{aligned} Y &= X^{\frac{n_1}{m_1}} + X^{\frac{n_2}{m_1 m_2}} + \dots + X^{\frac{n_i}{m_1 \dots m_i}} \\ &= X^{q_1} + X^{q_2} + \dots + X^{q_i} \end{aligned}$$

Consider a small circle $\mathbb{S}^1_\delta \subset \mathbb{C}$ and let $\mu : [0,1] \to \mathbb{S}^1_\delta$, $\mu(t) = \delta e^{2\pi i t}$ be a loop around the circle. At the initial point $X = \mu(0)$, the first term X^{q_0} corresponds to the m_1 roots of unity on a circle of radius δ^{q_1}. As t runs from 0 to 1, each of these points rotate $q_1 = \frac{n_1}{m_1}$ times around the origin.

For $q_2 = \frac{n_2}{m_1 m_2}$, the second term X^{q_2} adds m_2 points around each of the m_1 points determined by the first term, equally spaced around circles of radius $\delta^{q_2} < \delta^{q_1}$. By choosing $\delta > 0$ small enough, one can ensure that none of these smaller circles intersect; we will show this precisely in the next lemma. For example, with the first two Puiseux pairs being $(3,4)$ and $(4,17)$, the next figure illustrates the situation at $t = 0$.

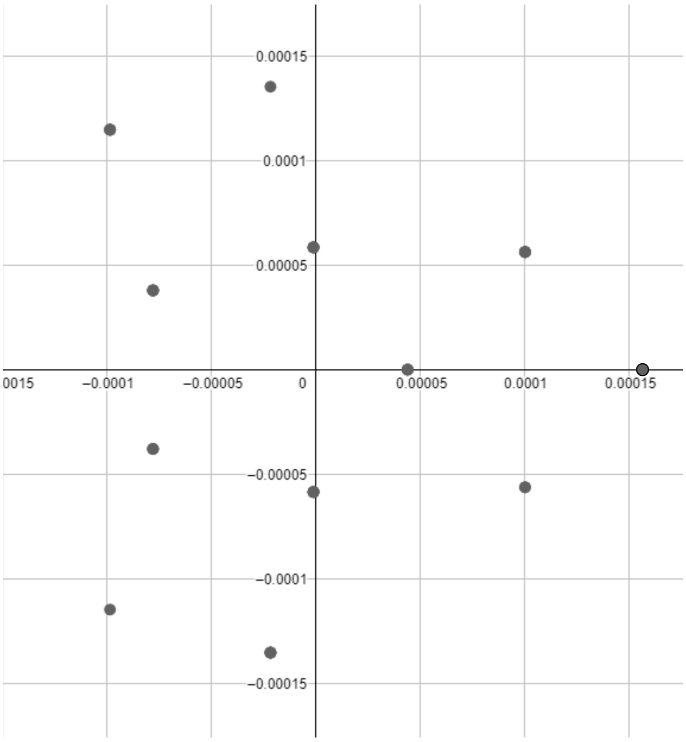


Image at $\delta = 0.001$, $t = 0$ of the standard expansion $X^{\frac{4}{3}} + X^{\frac{17}{3\cdot 4}}$, when considered as a multi-valued function.

As t goes from 0 to 1, the centres of the three smaller circles rotate $\frac{4}{3}$ times around the origin. Around each smaller circle, the four points each rotate $\frac{17}{12}$ times around their centre. Because t parametrizes a circle, the start and end states are glued together, and the result is a type of iterated braid of 12 individual "strings".

In general, this iterated braiding process continues for each term in the expansion. For $1 < j \leq i$, the term X^{q_j} determines $m_1 \dots m_j$ points in groups of m_j on circles of radius δ^{q_j} around the previous $m_1 \dots m_{j-1}$ points. Let us now prove that δ can always be chosen small enough such that these iterated circles never intersect, even if coefficients other than 1 are present.

Lemma 4.2.2. *Let $a_1, \dots, a_i \in \mathbb{C}\backslash\{0\}$ and $q_1 = \frac{n_1}{m_1}, \dots, q_i = \frac{n_i}{m_i}$ satisfy the conditions of Proposition 4.2.1. Then there exists $\delta_i > 0$ such that for all $0 < \delta < \delta_i$, the braid* *of $a_1X^{q_1} + \cdots + a_iX^{q_i}$ on $\mathbb{S}^1_\delta$ is well-defined in the sense that the iterated circles do not intersect.*

Proof. For each $n \in \mathbb{N},\ n \geq 2$, let $k_n > 0$ be the distance between two adjacent n:th roots of unity. Then $k_n \leq 2$ and on a circle of radius r, n equally spaced points along the perimeter are at least distance $k_n r$ from each other.

Set $r_1 = k_{m_1}|a_1|\delta^{q_1}$. Because $q_2 > q_1$, $|a_2|\delta^{q_2}$ shrinks faster than $|a_1|\delta^{q_1}$ as δ approaches 0, in the sense that $\frac{|a_2|\delta^{q_2}}{|a_1|\delta^{q_1}} = \left|\frac{a_2}{a_1}\right|\delta^{q_2-q_1}$ tends to 0. Hence there exists $\delta_1 > 0$ such that $|a_2|\delta^{q_2} < \frac{1}{4}r_1 = \frac{1}{4}k_{m_1}|a_1|\delta^{q_1}$ for all $0 < \delta < \delta_1$.

Set $r_2 = k_{m_2}|a_2|\delta^{q_2}$. Then $|a_3|\delta^{q_3}$ shrinks faster than both $|a_1|\delta^{q_1}$ and $|a_2|\delta^{q_2}$, so there exists $\delta_2 < \delta_1$ such that $|a_3|\delta^{q_3} < \frac{1}{4}r_2 = \frac{1}{4}k_{m_2}|a_2|\delta^{q_2}$ and $|a_2|\delta^{q_2} < \frac{1}{4}k_{m_1}|a_1|\delta^{q_1}$ for all $0 < \delta < \delta_2$.

Continuing this process, we have $r_j = k_{m_j}|a_j|\delta^{q_j}$ and ever faster shrinking functions $|a_j|\delta^{q_j}$. Eventually, we get a δ_i such that $|a_j|\delta^{q_j} < \frac{1}{4}|a_{j-1}|r_{j-1}$ for every $1 < j \leq i$ and $0 < \delta < \delta_i$. It remains to show that for such δ, none of the associated circles in the braid intersect.

Let $\delta \in (0, \delta_i)$. The points defined by $a_1X^{q_1}$ lie on a circle of radius $|a_1|\delta^{q_1}$, and these points are a distance at least r_1 from each other. The circles of radius $|a_2|\delta^{q_2}$ defined by $a_2X^{q_2}$ around these points have radius less than $\frac{1}{4}r_1$, so the distance between their perimeters is at least $\frac{1}{2}r_1$. In particular, since $r_2 = k_{m_2}|a_2|\delta^{q_2} < k_{m_2}\frac{1}{2}r_1 \leq \frac{1}{2}r_1$, the m_1m_2 points defined by $X^{q_1} + X^{q_2}$ lie at least distance r_2 from each other.

Inductively, the next term X^{q_j} defines $m_1 \dots m_j$ circles of radius less than $\frac{1}{4}r_{j-1}$, around points a minimum distance r_{j-1} from each other. Distance between the circles is at least $\frac{1}{2}r_{j-1}$, and since $r_j = k_{m_j}\delta^{q_j} < \frac{1}{2}r_{j-1}$, the new points are separated by at least r_j. By our choice of δ, this holds for every j i.e. the statement holds. $\square$

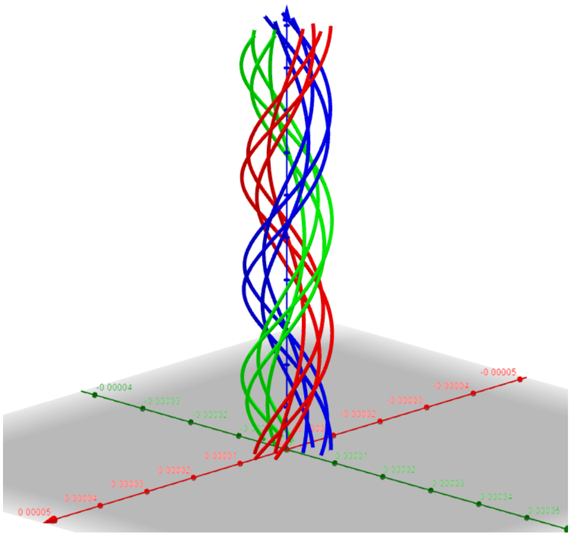
Now let us consider a braid not given by a standard expansion. Let

$$Y = X^{\frac{5}{4}} + X^{\frac{31}{4}}.$$

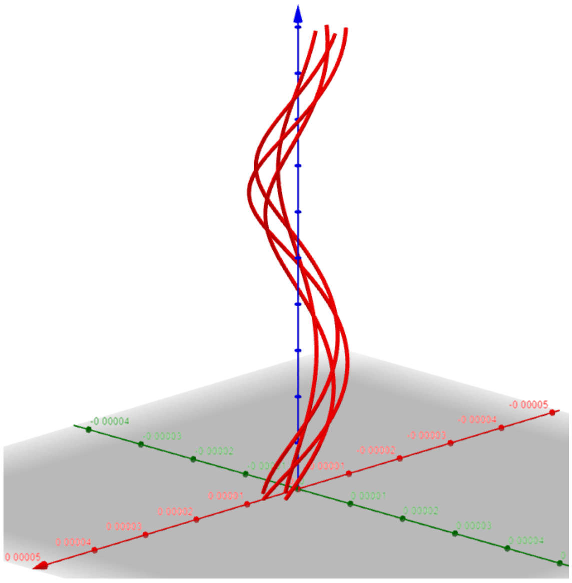
This expansion only has one Puiseux pair $(4, 5)$. The second term $X^{\frac{31}{4}}$ does not change the number of strings of the braid, but only adds small perturbations around the strings given by the previous term. These perturbations can be continuously "smoothed out", which yields the braid of the standard expansion of the pair $(4, 5)$. For example, letting $I = [0, 1]$ be the unit interval, the map

$$F : I \times I \to \mathbb{C},\ F(t, s) = \delta^{\frac{5}{4}}e^{2\pi i\frac{5t}{4}} + s \cdot \delta^{\frac{31}{4}}e^{2\pi i\frac{31t}{4}}$$

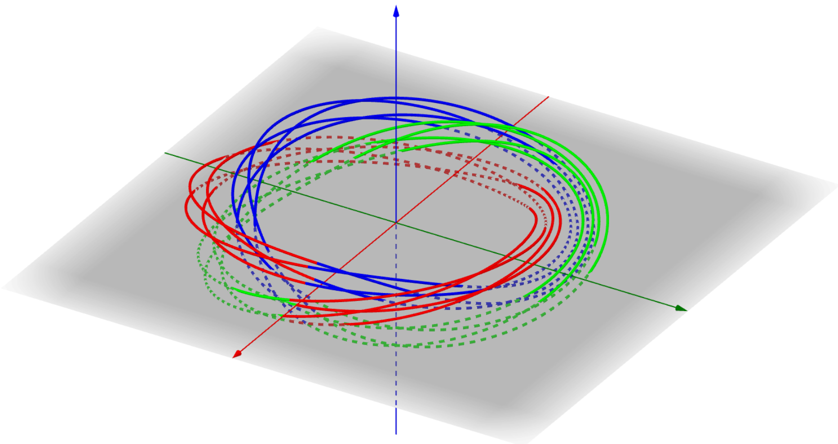
does this explicitly. It is continuous, and $F(t, 0)$, $F(t, 1)$ correspond to an individual string in $Y = X^{\frac{5}{4}}$ and $Y = X^{\frac{5}{4}} + X^{\frac{31}{4}}$ respectively. As s moves from 1 to 0 the latter is continuously deformed into the former. The map F is an example of a *homotopy* between two functions $I \to \mathbb{C}$.



As t runs from 0 to 1 on the Z-axis, $\mu(t)$ traces a circle and the expansion $X^{\frac{4}{3}} + X^{\frac{17}{3 \cdot 4}}$ on $\mu(t)$ forms a braid

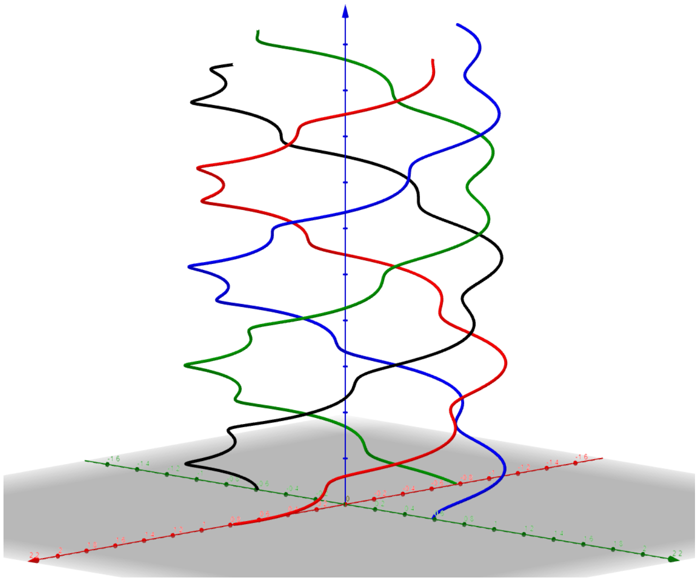


One of the three larger "threads" (groups of 4) plotted separately



The previous braid with ends glued together, embedded in $\mathbb{R}^3$. An example of a so-called iterated torus knot of type $(3,4),(4,17)$.

We would like to deform all the strings of a braid simultaneously, without them passing through each other at any point. For this purpose, let us re-frame our defini-



The braid of the expansion $X^{\frac{5}{4}} + X^{\frac{31}{4}}$ *at* $\delta = 0.73$

tion of a braid. For each natural number $m \geq 2$, define

$$U_m = \{(z_1, \ldots, z_m) \in \mathbb{C}^m \mid z_i \neq z_j \text{ for } i \neq j\}$$

Then e.g. $X^{\frac{5}{4}}$, considered a multi-valued function and evaluated at 1, yields the tuple

$$(1, e^{2\pi i \frac{5}{4}}, e^{2\pi i \frac{10}{4}}, e^{2\pi i \frac{15}{4}}) = (1, e^{\frac{1}{2}\pi i}, e^{\pi i}, e^{\frac{3}{2}\pi i}) \in U_4.$$

But so does $X^{\frac{n}{4}}$ for any n relatively prime to 4, possibly in different order. To make the order of strings in a braid irrelevant, we identify points in U_m whose coordinates are just permutations of each other. Specifically, the symmetric group S_m defines a group action on U_m by exchanging coordinates. Then we set

$$Y_m = U_m / S_m$$

with the quotient topology. For two m-tuples x and y, we have $x \sim y$ if and only if there exists $\sigma \in S_m$ such that $\sigma x = y$, i.e. one is a rearrangement of the other.

We define a *braid* with m strings as a closed path on Y_m, i.e. a continuous function $\mu : I \mapsto Y_m$ where $\mu(0) = \mu(1)$. Because the coordinates at any point are disjoint by definition of Y_m, we can recover our previous notion of the braid of a multi-valued function by taking the union of the projections from Y_m to $\mathbb{C}$.

Now a Puiseux expansion

$$\psi\left(X^{\frac{1}{m}}\right) = a_1 X^{\frac{n_1}{m}} + a_2 X^{\frac{n_2}{m}} + \cdots \in \mathbb{C}[[X^{\frac{1}{m}}]]$$

on a circle of radius δ defines the braid

$$\begin{aligned}
t \mapsto &\left(\psi\left(\delta e^{2\pi i \frac{t}{m}}\right), \psi\left(\delta e^{2\pi i \frac{t+1}{m}}\right), \dots, \psi\left(\delta e^{2\pi i \frac{t+m-1}{m}}\right)\right) \\
= &\Big(a_1 \delta^{\frac{n_1}{m}} e^{2\pi i \frac{n_1 t}{m}} + a_2 \delta^{\frac{n_2}{m}} e^{2\pi i \frac{n_2 t}{m}} + \dots, \\
&\quad a_1 \delta^{\frac{n_1}{m}} e^{2\pi i \frac{n_1(t+1)}{m}} + a_2 \delta^{\frac{n_2}{m}} e^{2\pi i \frac{n_2(t+1)}{m}} + \dots, \\
&\quad \vdots \\
&\quad a_1 \delta^{\frac{n_1}{m}} e^{2\pi i \frac{n_1(t+m-1)}{m}} + a_2 \delta^{\frac{n_2}{m}} e^{2\pi i \frac{n_2(t+m-1)}{m}} + \dots\Big)
\end{aligned}$$

We say two braids $\varphi, \psi : I \to Y_m$ are *equivalent*, if there exists a free homotopy between them; i.e. a continuous function $F : I \times I \to Y_m$ such that for all $t \in I$, $F(t, 0) = \varphi(t)$ and $F(t, 1) = \psi(t)$. We denote this $F : \varphi \simeq \psi$ for short, or simply $\varphi \simeq \psi$ if a homotopy is known to exist.

To better motivate the term *equivalent*, let us quickly verify that homotopy induces an equivalence relation on continuous functions with the same domain and codomain. In particular, $F(t, s) = \varphi(t)$ for all s, t gives a homotopy from φ to itself. If $F : \varphi \simeq \psi$, then $G : \psi \simeq \varphi$ where $G(t, s) = F(t, 1 - s)$. Finally, if $F : \varphi \simeq \psi$ and $G : \psi \simeq \theta$, define

$$H(t, s) = \begin{cases} F(t, 2s), \ 0 \le s \le \frac{1}{2} \\ G(t, 2s - 1), \ \frac{1}{2} \le s \le 1 \end{cases}$$

The two cases agree at $s = \frac{1}{2}$, and by the gluing lemma H is a continuous function. Then we have $H : \varphi \simeq \theta$, showing the transitivity of homotopy.

We now have the necessary machinery to say something about the topology of braids: that curves with the same Puiseux pairs create equivalent braids, in particular equivalent to that of their standard expansion. In a sense, the Puiseux pairs are invariants and provide us a way to classify singularities of irreducible curves by their associated braids.

Theorem 4.2.3. *Let $f \in \mathbb{C}[X, Y]$ be an irreducible plane curve with Puiseux expansion $\varphi(X) = \sum_q a_q X^q$. Let $\psi(X) = X^{q_1} + \cdots + X^{q_i}$ be the standard expansion of the Puiseux pairs $(m_1, n_1), \dots, (m_i, n_i)$ of φ. Then the braids of $\varphi(X)$ and $\psi(X)$ are equivalent.*

Proof. Write

$$\varphi = \tilde{\varphi} + \lambda,$$

where

$$\tilde{\varphi} = a_{q_1} X^{q_1} + \cdots + a_{q_i} X^{q_i}$$

consists of the terms corresponding to the Puiseux pairs, and λ contains all other terms. Then $\tilde{\varphi}$ and ψ differ only by their coefficients.

Like in the example seen before, the terms in λ not corresponding to Puiseux pairs do not change the number of strings, but only add perturbations. Thus they can be smoothed out by a homotopy, whereby φ and $\tilde{\varphi}$ are equivalent. The technical details of this part are given by Pham [3].

Set $m = m_1 \dots m_i$ and define $F : I \times I \to Y_m$,

$$F(t,s) = \left(\sum_{j=1}^{i} \frac{a_{q_j}}{1 - s + s\left|a_{q_j}\right|} \delta^{q_j} e^{2\pi i q_j t}, \dots, \sum_{j=1}^{i} \frac{a_{q_j}}{1 - s + s\left|a_{q_j}\right|} \delta^{q_j} e^{2\pi i q_j (t+m-1)} \right).$$

This homotopy continuously scales each coefficient to norm 1. Since the norms of $\frac{a_{q_j}}{1-s+s\left|a_{q_j}\right|}$ lie between $\left|a_{q_j}\right|$ and 1, by Lemma 4.2.2 one can choose δ small enough such that none of the circles intersect for these intermediary values. As such, the image is in Y_m and F is well-defined, where $F(t,0)$ is the braid of $\tilde{\varphi}$ and $F(t,1)$ is the braid of

$$\theta = \sum_{j=1}^{i} \frac{a_{q_j}}{\left|a_{q_j}\right|} X^{q_j}.$$

Now θ and the standard expansion ψ are the same, except their terms are rotations of each other. We may write

$$\theta = \sum_{j=1}^{i} e^{2\pi i \xi_j} X^{q_j},$$

where for each j, $0 \leq \xi_j < 1$. Now define

$$G(t,s) = \left(\sum_{j=1}^{i} \delta^{q_j} e^{2\pi i s \xi_j} e^{2\pi i q_j t}, \dots, \sum_{j=1}^{i} \delta^{q_j} e^{2\pi i s \xi_j} e^{2\pi i q_j (t+m-1)} \right),$$

where $G(t,0)$ and $G(t,1)$ are the braids of ψ and θ respectively. In the construction in the proof of Lemma 4.2.2, the rotation factor $e^{2\pi i s \xi_j}$ would not change the distance between points on the same circle, and the circle radii are the same. Hence also for $0 < s < 1$, the image of G is in Y_m i.e. $G : \psi \simeq \theta$ is a well-defined homotopy.

By the transitivity of homotopy, then the braids of φ and ψ are equivalent. $\square$

References

[1] E. Brieskorn, H. Knörrer. *Plane Algebraic Curves*. Birkhäuser, 1981. ISBN: 0-8176-3030-9.

[2] Ernst Kunz. *Introduction to Commutative Algebra and Algebraic Geometry*. 1933. ISBN: 3-7643-3065-1.

[3] F. Pham. *Singularités des courbes planes : Une introduction à la géométrie analytique complexe (Cours de 3e cycle, faculté des sciences de Paris, année universitaire 1969-1970)*. fre. Ecole polytechnique. Centre de Mathématiques, 1970.

[4] Gerd Fischer. *Plane Algebraic Curves*. 2001. ISBN: 0-8218-2122-9.

[5] M.F. Atiyah, I.G. Macdonald. *Introduction to commutative algebra*. 1969.

[6] P.W. Burau. *Algebraische Kurven der Ebene*. De Gruyter, 1962. ISBN: 978-3-11-136433-9.

[7] Pierre Samuel. "On unique factorization domains". In: *Illinois Journal of Mathematics* 5.1 (1961), pp. 1–17. DOI: `10.1215/ijm/1255629643`.

[8] Steven Dale Cutkosky. *Resolution of Singularities*. 2004. ISBN: 0-8218-3555-6.

[9] William Fulton. *Algebraic Curves*. 2008.